Project acronym:	PRISMS
Project title:	The PRIvacy and Security MirrorS: Towards a European framework for integrated decision making
Project number:	285399
Programme:	Seventh Framework Programme for research and technological development
Objective:	SEC-2011.6.5-2: The relationship between Human privacy and security
Contract type:	Collaborative project
Start date of project:	01 February 2012
Duration:	42 months

Deliverable 2.1: Preliminary report on current developments and trends regarding technologies for security and privacy

Authors:	Bas van Schoonhoven, Marc van Lieshout, Arnold Rosendaal (TNO)
Reviewers:	Rachel L. Finn (Trilateral); Michael Friedewald (Fraunhofer ISI)
Dissemination level:	Restricted to a group specified by the consortium
Deliverable type:	Report
Version:	1.0
Due date:	30 September 2012
Submission date:	28 February 2013

About the PRISMS project

The PRISMS project analyses the traditional trade-off model between privacy and security and devise a more evidence-based perspective for reconciling privacy and security, trust and concern. It examines how technologies aimed at enhancing security are subjecting citizens to an increasing amount of surveillance and, in many cases, causing infringements of privacy and fundamental rights. It conducts both a multidisciplinary inquiry into the concepts of privacy and security and their relationships and an EU-wide survey to determine whether people evaluate the introduction of security technologies in terms of a trade-off. As a result, the project determines the factors that affect public assessment of the security and privacy implications of a given security technology. The project uses these results to devise a decision support system providing users (those who deploy and operate security systems) insight into the pros and cons, constraints and limits of specific security investments compared to alternatives taking into account a wider society context.

Terms of use

Document history

Version	Date	Changes
1.0	27 February 2013	

SUMMARY

The PRISMS project analyses the traditional trade-off model between privacy and security and devises a more evidence-based perspective for reconciling privacy and security, trust and concern. A number of activities are employed in the project, including an analysis of security and privacy technologies (of which this deliverable is part), a policy assessment, a criminological analysis, a legal perspective, a discourse analysis of media attention to privacy, security and trust issues, an analysis of existing public opinion surveys, and a survey of citizens' privacy and security perceptions.

In this preliminary report we lay a foundation for the analysis of the role that technology plays in the dynamics between security and privacy, by providing an overview of the current developments and trends in security and privacy technologies and their interrelationships. Other activities in the project build upon this overview by analysing how users attribute meaning to a number of privacy and security technologies, and developing illustrative examples to be used in the survey. In addition, the technology and technological developments and interrelations discussed here play an important role in the analysis of policy discourse, the legal perspective, media attention to privacy and security issues, and the public opinion.

Based on an extensive literature study of technology roadmaps, reports, foresight and policy documents we assessed for a series of key technological domains the fit for privacy or security purposes of technologies in each domain, the impact of the use of these technologies in practice, and drivers and barriers in the development of technologies for security and privacy. The assessment outcomes of different technology domains fit for purpose and impact in practice is summarized in Table 1 below:

	Fit for purpose		**Impact in practice**	
Technology domain	**Security**	**Privacy**	**Security**	**Privacy**
Signal and information processing tech.	High	Average	Positive	Negative
Artificial intelligence and decision support	Average	Low	Positive	Neutral
Sensor equipment and Sensor technologies	High	Low	Positive	Negative
Human sciences	Average	High	Positive	Positive
Information security technologies	High	High	Positive	Positive
Navigation and tracking	High	Low	Positive	Negative
Biometrics	High	Low	Positive	Negative
Integrated platforms	Average	Low	Positive	Negative
Energy generation, storage and distribution	Average	Low	Positive	Negative
Privacy protection	Average	High	Negative	Positive

Table 1 - overview of technology domains assessment on fit for purpose and impact

In this table a trade-off is visible between security and privacy that appears to be inherent in technology development and use. Increased investments in technologies that have a positive impact on security tend to simultaneously have a negative impact on privacy. Some notable exceptions exist, however: the fields of information security and human sciences do not show such a trade-off. A trade-off between privacy and security is also visible with regards to privacy protection technologies, especially when it comes to security by internet surveillance. Technologies specifically developed to enhance anonymity and to secure communications (showing an overlap with the information security domain) are perceived by some reports as having a negative impact on security through surveillance.

Technology development is subject to factors that drive it or hinder it, influencing how the trade-off between security and privacy turns out. We performed a preliminary analysis of the drivers and barriers that respectively drive security and privacy technological developments, or act as barriers to these developments. The drivers and barriers outlined here are based on a literature study of policy documents, technology roadmaps, foresight studies and impact assessments. An overview of the drivers and barriers that were identified is provided in Table 2 and Table 3.

Driver	Effect on technology development for security	Effect on technology development for privacy
Technology and industry push	Strong	Weak
Events with high societal impact	Strong	Weak
Government policy and regulation	Strong	Strong
Consumer demand	Strong	Strong

Table 2 – factors driving technology development and use

Barrier	Effect on technology development for security	Effect on technology development for privacy
Lack of standardization	Strong	Strong
Not a unique selling point	Average	Strong
Reactive approach	Average	Strong

Table 3 – factors hindering technology development and use

Overall these tables suggest that technology development for security is subject to a number of drivers that are mostly absent for privacy: a technology and industry push, and events with a high societal impact. In addition, the relatively new field of privacy protection technologies suffers from a number of barriers that are less pronounced in the more established fields of security protection technologies: the idea that privacy is not a unique selling point, and a mostly reactive approach to the use of such technologies by consumers and organizations.

One of the end results of the PRISMS project is a decision support system that will provide users (those who deploy and operate security systems) insight into the pros and cons, constraints and limits of specific security investments compared to alternatives taking into account a wider society context. While this preliminary analysis lacks nuance and detail, we identified a starting point for a decision support system on investments in security and privacy technologies, which may be based on the summarizing tables on technology domains, drivers and barriers listed above.

The results described in this deliverable are preliminary; based on the other activities performed in the same work package and in other work packages the results will be improved further, and eventually integrated into a final report on current developments on security and

privacy technologies including studies on the mutual shaping processes between developers, users and uses of security and privacy technologies. With this preliminary deliverable we lay a foundation for the work done in the other activities in the PRISMS project that often relate to technology, including a policy assessment, a criminological analysis, a legal perspective, a discourse analysis of media attention to privacy, security and trust issues, an analysis of existing public opinion surveys, and a survey of citizens' privacy and security perceptions.

CONTENTS

1 INTRODUCTION

The PRISMS project analyses the traditional trade-off model between privacy and security and devises a more evidence-based perspective for reconciling privacy and security, trust and concern. It examines how technologies aimed at enhancing security are subjecting citizens to an increasing amount of surveillance and, in many cases, causing infringements of privacy and fundamental rights. It conducts both a multidisciplinary inquiry into the concepts of privacy and security and their relationships and an EU-wide survey to determine whether people evaluate the introduction of security technologies in terms of a trade-off. One of the end results of the project is a decision support system providing users (those who deploy and operate security systems) insight into the pros and cons, constraints and limits of specific security investments compared to alternatives taking into account a wider society context.

In order to achieve these results, a number of activities are employed in the project, including an analysis of security and privacy technologies (of which this deliverable is part), a policy assessment, a criminological analysis, a legal perspective, a discourse analysis of media attention to privacy, security and trust issues, an analysis of existing public opinion surveys, and a survey of citizens' privacy and security perceptions.

Technology plays a central role in the dynamics involved in security and privacy. This deliverable lays a foundation of the analysis of the role that technology plays by providing an overview of the current developments and trends in security and privacy technologies and their interrelationships. Other activities in the project build upon this overview by analysing how users attribute meaning to a number of privacy and security technologies, and developing illustrative examples to be used in the survey. In addition, the technology and technological developments and interrelations discussed here play an important role in the analysis of policy discourse, the legal perspective, media attention to privacy and security issues, and the public opinion.

This preliminary report starts with discussing in chapter 2 the approach taken in the task that has this deliverable as its result. Chapter 3 continues by introducing some central concepts that are relevant in our discussion on technologies and their interrelations. This is followed by the core part of the deliverable: chapter 4, which identifies a series of technological domains, the fit for privacy or security purposes of technologies in the domains, the impact of the use of these technologies in practice, and drivers and barriers involved in technology development for security and privacy. Based on this analysis, the central conclusions are drawn in chapter 5.

The outcomes of this deliverable will be integrated into the final deliverable of work package 2 of the PRISMS project, together with the outcomes of a socio-technical analysis of several technologies, and the results of on-going monitoring of technological developments.

2 APPROACH

The main aim of task 2.1 is to provide an overview of current developments and trends in security and privacy technologies and their interrelationships. In this report we focus primarily on security technologies, while developments in privacy technologies are discussed to the extent that they affect security issues.

The approach taken in this task consists of a number of different and connected activities:

1. **conceptual analysis**: outlining the concepts of "technology", "security technology", and "privacy technology";

2. **literature review** of relevant technology reports, technology foresight documents, technology impact assessments and technology roadmaps;

3. **identification of key technologies** for privacy and security based on the literature review;

4. basic **data mining** of European research project descriptions relating to security or privacy to discover trends and relations between (technology) concepts; and

5. **analysis** of relevant security and privacy technologies, their impacts, recent technical developments, and drivers and barriers to these developments.

The approach taken in each of these activities will be briefly discussed below.

2.1 CONCEPTUAL ANALYSIS

As a starting point of the PRISMS project, we discussed the definitions of security and privacy in some detail in the first deliverable.[1] We use these definitions as a starting point for the conceptual analysis in this report. Since there are risks involved in talking about 'technology' as if it were a monolithic thing, we refine our definition of technology by splitting technologies up into building blocks, systems, and systems of systems while trying to avoid talking about 'technology' in general. Also, we broaden our perspective from technology to the way meaning is assigned to technologies in practice and in society by using the Science & Technology Studies concepts of *inscription*, and *social shaping of technology*.

2.2 LITERATURE STUDY

In the literature study we used a number of different sources in order to identify relevant documents:

- websites of EU organizations such as CORDIS, ENISA, the European Foresight Platform, the European Commission, and the European Parliament;

- academic article databases (e.g. SSRN, IEEE);

[1] Friedewald, Michael, David Wright, Kush Wadhwa, et al., "Central Concepts and Implementation Plan", PRISMS Deliverable 1.1, 2012.

- internet search engines (e.g. Google);
- input from neighbouring projects (in particular PACT and SurPRISE);
- references in documents collected.

Since it was not feasible to scan through *all* security or privacy technology related reports and documents ever written, the focus for this search was on high-level discussions, such as technology roadmaps, policy discussions, large-scale research projects, impact assessments and foresight studies, with a preference for recent publications. We used quick, manual scans to determine the relevance of documents found using keyword searches were. These manual scans were based on a commonly shared template format. This template is included in appendix A for reference. The complete list of documents that were reviewed is included in appendix B.

2.3 DATA MINING

Considering the large number of research projects carried out in the EU programmes (numbering in the tens of thousands), manually scanning these projects outputs for security and privacy developments was also not feasible. However, in addition to the focused literature study, we conducted a data mining exercise on the basis of suitable keywords identified during the literature study. The key assumption behind this data mining effort was that objective descriptions of the European Framework programmes are a reliable proxy for descriptions of activities in the field of security and privacy technologies. The goal of the data mining approach was to identify trends in keyword usage (e.g. increasing or decreasing use of 'surveillance' combined with 'privacy' as part of project descriptions).

Projects in the following EU research programmes were targeted in the data mining activity:

- Preparatory Action for Security Research (PASR)
- Seventh Framework Programme (FP7)
- Sixth Framework Programme (FP6)
- Fifth Framework Programme (FP5)

The CORDIS website (http://cordis.europa.eu) lists all EU framework programme projects in a consistent manner, and was used as the source of texts to mine. The data mining approach consisted originally of the following steps:

1. Search CORDIS using its 'advanced search' feature. Three searches were performed:
    a. Programme Acronym: FP7, search all fields for 'privacy' OR 'security'. *This resulted in 1074 projects found*
    b. Programme Acronym: FP6, search all fields for 'privacy' OR 'security'. *This resulted in 505 projects found*
    c. Programme Acronym: FP5, search all fields for 'privacy' OR 'security'. *This resulted in 413 projects found*

2. Creating a list of CORDIS project page web-addresses based on these results.

3. Automated "crawling" of these web-addresses to collect data on each to be used during the data mining: project title, objective, programme acronym, start date, duration in months, cost in Euro, link to its CORDIS page. The data resulting from this automated crawl was the main corpus used for data mining.

4. A series of data mining exercises on this corpus (i.e., project descriptions which already use either the word 'security' or 'privacy'):

    a. Counting 'privacy' and 'security' keyword usage in project objectives over the years.

    b. Counting 'mission' keyword usage in project objectives over the years. Mission keywords that identify some overall EU security mission objectives (which have undergone some changes over time): for example, critical infrastructure, security in times of crisis, border security, and fighting terrorism and organized crime.

    c. Counting keyword usage of some key capabilities: detection, identification, surveillance.

    d. Counting correlating occurrences of a set of keywords (e.g., how often 'surveillance' is used together with 'privacy').

5. The results of this data mining were post-processed (e.g., corrections for the changes in the # of projects over time).

6. We manually scanned results for correctness (e.g., did the chosen keywords used in objective descriptions as was thought, or were they used in another meaning?). A number of iterations of the data mining were performed, each time with adjusted keywords based on this manual check.

One issue with this approach turned out to be that many keywords that were originally envisioned as suitable (e.g., 'ANPR' or 'automated number plate recognition') were not used at all in the high-level objective descriptions of the CORDIS database. One way to work around this would have been to expand the corpus with more detail, e.g., include all reports of the relevant studies. However, the effort involved would have been prohibitive, since the reports are not always presented in a consistent manner or format, and the amount of data that would need to be processed would exceed the technical possibilities currently available. Instead, we decided to manually scan the results of keyword relevance, to use more generic terms where possible, and to adjust the keywords used in a number of iterations to improve the results.

2.4 ANALYSIS

In this phase of the analysis, we combined and analysed the results of the literature study and the data mining. This phase of the analysis identified key security and privacy technologies, and discussed trends, impacts and foresights. The outcome of this analysis is discussed in chapters 4, and the conclusions are presented in chapter 5.

3 CORE CONCEPTS

In order to understand the meaning of technological developments in security and privacy technologies, the core concepts used to shape our understanding must be clarified. These concepts include of course "security" and "privacy". The definition of these two concepts we use in this report is based the discussion provided in PRISMS deliverable D1.1. In this chapter, the meaning of the terms 'privacy technology' and 'security technology' are also discussed, along with how to bring some much-needed nuance in the use of this concept. The conceptual discussion follows two lines: first, distinguishing between "building blocks", "systems", and "systems of systems", and second, by recognizing the importance of discussing technologies in (social) context, especially when relating to systems or systems of systems. For the second line of enquiry, we introduce the concepts of 'inscription' and 'sociotechnical arrangements'.

3.1 SECURITY

As discussed in PRISMS deliverable D1.1, the European Committee on Standardisation's working group 161 provides a mainstream definition of security :

> *security is the condition (perceived or confirmed) of an individual, a community, and organisation, a societal institution, a state, and their assets (such as goods, infrastructure), to be protected against danger or threats such as criminal activity, terrorism or other deliberate or hostile acts, disasters (natural and man-made).*[2]

Security as a concept is multidimensional, and generally defined in a very broad sense. It relates to many different scales: international security, national security, corporate security, societal security, and individual security. For the PRISMS project, societal and individual scale are primarily relevant.

The concept of security is also multidimensional with regards to *what* the main asset or value is that is thought to be (in)secure. Deliverable D1.1 provides a preliminary taxonomy of security, which distinguishes between a number of different dimensions with regards to the *what* of security:

1. **Physical security**: concerned with physical measures designed to safeguard the physical characteristics and properties of systems, spaces, objects and human beings.

2. **Political security**: concerned with the protection of acquired rights, established institutions/structures and recognized policy choices.

3. **Socio-Economic security**: concerned with economic measures designed to safeguard the economic system, its development and its impact on individuals.

4. **Cultural security**: concerned with measures designed to safeguard the permanence of traditional schemas of language, culture, associations, identity and religious practices.

[2] Martí Sempere, Carlos, "The European Security Industry: A Research Agenda", Economics of Security Working Paper 29, German Institute for Economic Research, Berlin, 2010.

5. **Environmental security**: concerned with measures designed to provide safety from environmental dangers caused by natural or human processes.

6. **Radical uncertainty security**: concerned with measures designed to provide safety from exceptional and rare violence/threats, which are not deliberately inflicted by an external or internal agent, but can still threaten drastically to degrade the quality of life.

7. **Information security**: concerned with measures designed to protect information and information systems from unauthorized access, modification or disruption.[3]

3.2 PRIVACY

The concept of privacy has a long history and it has been defined in many ways. Back in 1890, Warren and Brandeis defined it as "the right to be let alone".[4] In 1967, the influential privacy researcher Alan Westin described it as "an instrument for achieving individual goals of self-realization" and "the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others".[5]

More recently, researchers have recognized that privacy is a concept that is impossible to fully define in a single definition, and that there are multiple dimensions to privacy, for example as argued by Daniel Solove in his book "Understanding Privacy".[6] Solove differentiates between different dimensions of privacy according to the type of privacy invasions, e.g. surveillance, aggregation, or intrusion. However, the outlining of privacy problems or intrusions does little to provide an overarching framework that would ensure that individuals' rights are proactively protected.

Rights to privacy, such as those enshrined in the European Charter of Fundamental Rights, require a forward-looking privacy framework that positively outlines the parameters of privacy in order to prevent intrusions, infringements and problems. Recently, a conceptualisation of privacy as seven types of privacy, have been identified by Finn, Wright, and Friedewald:

1. **Privacy of the body**: the right to keep body functions and body characteristics (such as genetic codes and biometrics) private.

2. **Privacy of behaviour**: the right to keep actions and behaviour private, including sensitive issues such as sexual preferences and habits, political activities and religious practices.

3. **Privacy of communication**: the right to avoid the interception of communications.

[3] Friedewald, et al., 2012.
[4] Warren, Samuel D. and Louis D. Brandeis, "The Right To Privacy", *Harvard Law Review*, Vol. 4, No. 5, 1890, pp. 193-220.
[5] Westin, Alan F., *Privacy and freedom*, Atheneum, New York, 1967.
[6] Solove, Daniel J., *Understanding privacy*, Harvard University Press, Cambridge, Mass., 2008.

4. **Privacy of data and image**: the right to protection of an individual's data from being automatically available or accessible to other individuals and organisations and ensuring that people can exercise a substantial degree of control over that data and its use.

5. **Privacy of thoughts and feelings**: the right not to share thoughts or feelings or to have those thoughts or feelings revealed.

6. **Privacy of location and space**: the right to move about in public or semi-public space without being identified, tracked or monitored.

7. **Privacy of association**: the right to associate with whomever they wish, without being monitored.[7]

3.3 TECHNOLOGY

The term 'technology' stems from two Greek words: *techne* and *logos*. *Techne* refers to the work of craftsmen that are capable of producing arts which may serve as a means to a specific end.[8] The term '*techne*' is closely related to the term '*épistêmê*' which refers to the ancient Greek approach of scientific knowledge (being knowledge related to abstract and invariable knowledge fields, such as geometry). *Techne* refers to scientific knowledge which the craftsmen possess for the production of objects ('artefacts') which serves as means for a specific end ('know how'). Producing a chip, for instance, as a means to enable calculations being done automatically is an example of this. To be able to produce a chip requires systematic knowledge on practical issues which have some level of universal appeal. One has to take account of theoretical approaches as laid down in quantum physics, but at the same time one needs also be aware of the practical implications of quantum physics in reality and of practical implications of working in clean rooms that still allow some dust (however small). The term *logos* refers to the ability to calculate about actions, i.e. being rational about them. In that sense, the term *technology* as it is described in the Webster dictionary is still very indebted to the ancient Greek philosophers, of which especially Aristotle is closest to our common understanding of the word.[9]

The Webster dictionary discerns between three meanings of technology:

1. Technology is
   a. The practical application of knowledge especially in a particular area
   b. A capability given by the practical application of knowledge ('a car's fuel saving technology')
2. A manner of accomplishing a task especially using technical processes, methods or knowledge ('new technologies for information storage')
3. The specialized aspects of a particular field of endeavour ('educational technology') [10]

---

[7] Finn, Rachel L., David Wright and Michael Friedewald, "Seven types of privacy", in Gutwirth, Serge, et al. (eds.), *European Data Protection: Coming of Age*, Springer, Dordrecht, 2013.
[8] Parry, Richard, "Episteme and Techne", in Zalta, Edward N. (ed.), *The Stanford Encyclopedia of Philosophy (Fall 2008 Edition)*, Stanford, Cal., 2007.
[9] Ibid.
[10] Retrieved from http://www.merriam-webster.com/dictionary/technology

This definition encapsulates the definition as presented above (the application of knowledge to achieve a given end for a means) but adds issues such as process and methods. The application of "technical" knowledge may be understood as John Kenneth Galbraith stated in his influential definition: "the systematic application of scientific or otherwise organized knowledge to practical tasks".[11] In this report the term 'technology' is primarily used to refer to a manner of accomplishing a task using especially using technical processes, methods or knowledge.

The 2006 European Security Research Agenda distinguishes between three research paths: development of enabling technology, system development, and demonstration of systems of systems.[12] In our discussion on technological developments we use a division based on these research paths to distinguish between different levels of technology:

- **Building blocks**: basic enabling technologies and technological components that are useable for several purposes generic, e.g., sensor technologies or encryption algorithms. Building blocks may be clustering around technology domains.

- **Systems**: the smallest complete assembly of technologies and processes that together lead to an ability to perform a specific function, task or operation, e.g., remote detection of shipping containers, or access control to a web service. Systems may be clustered around functional groups (e.g., detection, identification and authentication).

- **Systems of systems**: a combination of different systems for an overarching purpose. For example, combining body scanners, camera surveillance, passenger record analysis and other technological systems into one system of systems that aims to provide airport security. Systems of systems are few in number, and may be identified by their overarching mission, e.g., border security for the EU.

Of course, any such a division of technologies is not flawless, as most "enablers" may also be conceptualized as "systems", and vice versa. However, the division is clear enough to help structure the analysis in the later chapters.

3.4 Security Technology and Privacy technology

In the previous discussions the terms 'security technology' and 'privacy technology' were used repeatedly. However, in reality, it is quite difficult to meaningfully distinguish "privacy technology" from "security technology". Since, technology is considered to refer to a manner of accomplishing a task, 'security technology' is defined as a technology used to enhance security. Identically 'privacy technology' is defined as a technology used to enhance privacy.

However, in many cases, the same technology can be used to enhance both security and privacy. For example, one of the most basic technologies, the door, is a good example of a technology that may be both a privacy and a security technology. Doors in a house protect rooms and the home environment itself from unwanted invasion of the privacy of the home. However, at an airport, doors block access for unauthorized individuals to certain areas in

[11] Galbraith, John Kenneth, *The New Industrial State*, Houghton Mifflin, Boston, 1971.
[12] ESRAB (European Security Research Advisory Board), "Meeting the challenge: the European Security Research Agenda. A report from the European Security Research Advisory Board", Office for Official Publications of the European Communities, Luxembourg, 2006.

order to increase security. Information cryptography is a technology that is often used to enhance privacy (e.g. by encrypting private messages), but simultaneously by enhancing security (also by encrypting private messages, or for implementing secure access control).

Therefore, a "security technology" can at the same time be a "privacy technology", or a "privacy and security technology", making these categories less useful in facilitating a clear discussion on these technologies and how they interrelate. Similarly, the concept of a Privacy Enhancing Technology (PET) is not useful to distinguish a specific category of technologies, it merely indicates a specific *usage* of technologies. Of course, some technologies are better fit for this usage than others; we will discuss this aspect of technology in the following section that relates to *inscription*.

3.5 Inscription and Fit for Purpose

The notion of inscription refers to the way technical artefacts embody patterns of use: "Technical objects thus simultaneously embody and measure a set of relations between heterogeneous elements".[13] This does not mean to suggest that action would be somehow hard-wired into an artefact. Instead, an artefact on one hand has an objective element in which it determines its use, and on the other hand a subjective element in which an artefact is interpreted and used flexibly by a subject.

Another way to conceptualize this is by recognizing that artefacts or technologies may be more or less *fit for purpose*, or *fit for use*. With "fit" we mean that a technology is effective in performing a specific task, e.g. a technology may be fit for enhancing security, and/or it may be fit for enhancing privacy. The pattern of use embodied in technological artefacts may be a good fit with one specific purpose, yet not exclude the use of the artefact for other purposes. For example, a surveillance camera is a good "fit" for enhancing security in public or private spaces, and not such a good fit for enhancing privacy (although such use could be envisioned, e.g., by a celebrity utilizing camera surveillance to protect his or her privacy of the home).

Previously we discussed how technology may be defined at different levels: that of building blocks, systems, and systems of systems. In general, building blocks allow for relatively many different uses, while systems of systems are designed, operated and used for one, or few purposes. Indeed, a system is defined as the smallest complete assembly of technologies and processes that together lead to an ability to perform a specific function, task or operation. In a different assembly, the same technologies may be used to perform an entirely different function. The level of inscription (i.e., the level to which technical artefacts embody patterns of use) often increases with the level of technology.

3.6 Social Shaping of Technology

A complementary perspective to inscription by technology is the social shaping of technology.[14] The social shaping of technology builds upon the philosophical and reflexive approach towards technology as an entity that is not fixed and invariable but that is open to change and re-interpretation, depending on societal perspectives. On the other hand, the social

[13] Akrich, Madeleine, "The description of technical objects", in Bijker, Wiebe and John Law (eds.), *Shaping Technology/Building Society: Studies in Sociotechnical Change*, MIT Press, Cambridge, Mass, 1992.
[14] Ibid.

shaping of technology presumes as well that society is shaped by technology and that specific technological manifestations have an impact upon society, upon traditions, rituals and habits.

The social shaping approach (also known as the mutual shaping of technology and society, or the co-construction of users and technology[15]) opens 'the black box' of technology and shows how specific technological instances are the product of interactions between technology developers, technology itself, and stakeholders that have a say in either the production or the use of technology. The stakeholders are of various kinds: users of products, standardisation bodies, policy makers, industrial boards, etc. They introduce factors in decision making processes around technology development which are typically different from pure technological motivations (such as striving for the most efficient or effective approach).

Clear examples emerge from the way IT-specialists try to understand the habits and attitudes of users in order to offer them products that align with their (cultural and societal) predispositions. However, at the same time these users are heavily influenced by what is presented as the latest and most novel gadgets. Devices such as modern tablet computers demonstrate this mutual shaping perspective. While designers and developers determine how the artefact will look and what functionalities will be offered in what manner, the different uses of the tablets help shaping follow-up generations (such as the introduction of a variety of platforms in different sizes and with different features for different functionalities). Another well-known example is the mutual shaping between societal practices and mobile telecommunications. Societal attitudes towards the frontier between work and private life, or towards what it means to be in reach have been influenced by developments in mobile telecommunications.[16] At the same time, the shaping of standardisation processes in mobile phones are not the sole result of technological considerations (striving to the most efficient approach for instance), but have been influenced by political and socio-economic considerations as well.[17]

The social shaping approach assists researchers in avoiding a perspective that is either technological deterministic in appearance (presuming technology is a force by itself, impacting upon society and influencing society by the mere manifestation of its course of events – which is uniquely led by technological factors) or socially deterministic (presuming whatever technology is developed it is the autonomous force of society that in the end determines what will be accepted). The position adopted is a compromise: technology clearly has some in-built features which are primarily determined by technological factors but principally it will always be the result of interaction of different actors with the technological environment that will give rise to specific dynamics.

One famous example may suffice to demonstrate the argument, which is 'Moore's law'. This 'law' was nothing more but a prediction by Gordon E. Moore, one of the founders of Intel, done in 1965, in which he predicted that the number of micro-chips on a transistor would

[15] Oudshoorn, Nelly and Trevor Pinch (eds.), *How Users Matter: The Co-Construction of Users and Technology*, MIT Press, Cambridge, Mass. and London, 2003.
[16] Green, Nicola, "On the Move: Technology, Mobility and the Mediation of Social Time and Space", *The Information Society: An International Journal*, Vol. 18, No. 4, 2002, pp. 281–292.
[17] Jo, Whasun, "Global Political Economy of Technology Standardization: A Case of the Korean Mobile Telecommunications Market", *Telecommunications Policy*, Vol. 31, No. 2, 2007, pp. 124–138.

double every year.[18] His prediction was based on observations of the past. His statement was put in a law in the early 1970's by a colleague (Carver Mead). Moore adapted his own prediction to a doubling of every two years in 1975, and another Intel executive (David House) added that the performance of chips (being the combination of the number of chips times their performance) would double every two years. Since then, industry has turned this statement into a 'law' that forced them to realize it in due time.[19]

[18] Moore, Gordon E., "Cramming More Components Onto Integrated Circuits", *Electronics*, Vol. 38, No. 8, 1965, pp. 114-117.

[19] van Lente, Harro and Arie Rip, "Expectations in Techological Developments: An Example of Prospective Structures to Be Filled in by Agency", in van der Meulen, Barend and Cornelis Disco (eds.), *Getting New Technologies Together: Studies in Making Socio-technical Order*, de Gruyter, New York, 1998.

4 TECHNOLOGIES FOR SECURITY AND PRIVACY

As discussed in chapter 2, technologies cannot be clearly separated into 'privacy technologies' and 'security technologies', especially so for basic enabling technologies (building blocks). Many technologies can be used both for enhancing security and for enhancing privacy, although some technologies are a better fit for one use than for the other.

The PRISMS project aims at analysing the traditional trade-off model between privacy and security, and devise a more evidence-based perspective for reconciling privacy and security, trust and concern. In this deliverable we lay a foundation for the activities required to analyse the trade-off model by assessing a number of technology domains that yield technologies useable to enhance security and privacy. More specifically, our analysis focuses on the fit for use of technologies for privacy and security purposes, and how the technologies impact security and privacy when used in practice. The primary focus of our assessment is in bringing trade-offs between security and privacy in relation to technologies to light.

We performed the analysis on two main technology levels: building blocks and the systems in which these building blocks are used. The analysis is based on a series of technology reports and technology roadmaps examined during the literature study. The number of security technologies is practically limitless and extremely varied, considering how broad the concept of security is: it includes diverse domains such as food safety, environmental security, preserving culture, protection against terrorism, or economic security. Based on the discussion on security in PRISMS D1.1, we focus on technologies that are used for enhancing individual security or privacy, or societal security.

Our approach to mapping trends in European research with regards to privacy and security is based on a basic data mining exercise on CORDIS project objective descriptions on the occurrence of specific keywords. We present the results of three data mining efforts in this chapter: the use of the keywords 'privacy' and 'security' over time, the use of keywords relating to the EU security missions over time (e.g. border security, fighting organized crime and terrorism), and finally keywords relating to three key security capabilities: 'detection', 'identification', and 'surveillance'.

The outcomes of the analysis described in this chapter (and the conclusions drawn in chapter 5) inform the other work packages in the PRISM project about the technologies that play a role when assessing privacy and security issues, for example during the analysis of policy documents, media perception, and the public opinion.

4.1 BUILDING BLOCKS & SYSTEMS

As discussed earlier, many (if not all) building blocks are technologies that are useable both for enhancing security and privacy. Building blocks may be assembled into a system that aims to either protect security or privacy, or to protect security while preserving privacy. In this section we discuss a series of key building block technologies according to their technological domain. Technologies can be divided into domains in many different ways; here a division

into technological domains is based on the one used in the European Security Research Agenda.[20]

Table 4 lists technology domains, along with a number of examples of key building blocks and systems in this domain. Some technology domains are relevant from a security perspective, but not interesting for a discussion on the interrelation between privacy and security technology, e.g., rapid analysis of biological agents, or electrical generators. We discuss the technology domains that have both a positive or negative impact on security and privacy in more detail. The relevant domains are highlighted in bold.

Technology domain	Building blocks for security or privacy
Signal & information processing technologies	Data fusion techniques, data collection/data classification, image/pattern processing technology, information fusion technology, data and information management technology, text mining / data mining, automatic number plate recognition
Artificial intelligence and decision support	IKBS/AI/expert techniques, knowledge management, modelling and simulation, optimisation and decision support technology
Sensor equipment	Cameras, radar sensor equipment, NRBC sensors (in particular biological and chemical threat detection technologies), passive IR sensor equipment, body scanners, subsurface scammers
Sensor technologies	Hyper spectral/multispectral sensors, hyper spectral/multispectral processing, autonomous small sensors/smart dust technologies, IR sensor technologies, Terahertz sensors, optical sensors technologies, acoustic sensors — passive, deep packet inspection (DPI)
Communication equipment	Reconfigurable communications, mobile secured communications, communications network management and control equipment, network supervisor, network and protocol independent secured communications, information security, secured, wireless broadband data links for secured communications, protection of communication networks against harsh environment
Social sciences and humanities	Human behaviour analysis and modelling, population behaviour, human factors in the decision process, teams, organisations and cultures
Information security technologies	Encryption and key management, data-mining, access control, filtering technologies, authentication technologies, encryption technologies (cryptography)
Computing technologies	Protocol technology, SW architectures, secure computing techniques, high performance computing, high integrity and safety critical computing, software engineering
Information warfare/intelligence systems	Infrastructure to support information management and dissemination, cyber security policy management tools, optimisation, planning and decision support systems
Scenario and decision simulation	Impact analysis concepts and impact reduction, advanced human behaviour modelling and simulation, simulation for decision making (real time simulation), structures vulnerability prediction, evacuation and consequence management techniques, mission simulation

[20] ESRABESRAB (European Security Research Advisory Board), 2006.

Technology domain	Building blocks for security or privacy
Information systems	Infrastructure to support information management and dissemination, cyber security policy management tools, optimisation, planning and decision support systems
Navigation and tracking	RFID tags, tracking, GPS, radio navigation, direction finding and map guidance, bar code based tracing, GSM triangulation
Biometrics	Fingerprints recognition (digital fingerprints), facial recognition, iris/retina, voice, handwriting, signature reconnaissance
Integrated platforms	UAVs (air/land/sea), lighter than air platforms, surveillance and navigation satellites
Survivability and hardening technology	EMC evaluation and hardening, smart clothes and equipment, anti-blast glasses/concretes, etc., critical buildings specific architectures, blast and shock effects
Electronic authentication	Electronic tagging systems, smart cards
Biotechnology	Rapid analysis of biological agents and of human susceptibility to diseases and toxicants, decontamination techniques, water testing and purification techniques, food testing and control techniques
Simulators, trainers and synthetic environments	Virtual and augmented reality, tactical/crew training systems, command and staff training systems, synthetic environments
Chemical, biological and medical materials	Chemical and biological detection techniques
Signal protection (warfare)	Non-cooperative target recognition, geographic information systems
Space systems	Earth observation (image and communications)
Light and strong materials, coatings	Light materials for human protection, smart textiles, light materials for site protection, self-protective and explosive resistant material technology, surfaces treatments for improvement of life duration, corrosion reduction
Energy generation, storage and distribution	Electrical generators, electrical batteries, energy distribution, secure smart grids
Privacy protection	Anonymisation, zero knowledge proofs, mix networks, onion routing, privacy by design, control and transparency tools for users

Table 4 - Technology domains and building blocks, based on the European Security Research Agenda (2006) expanded with some building blocks and the privacy protection domain. Domains with high estimated impact on both privacy and security are highlighted in bold.

As noted in the European Security Research Agenda, information and communication technologies stand out in this table. Technologies for gathering, storing, processing, displaying, using, communicating, and managing information are becoming ever more pervasive and revolutionize the manner in which organisations address their security needs.[21] The developments in information and communication technologies are tightly intertwined

[21] Ibid.

with other key security and privacy technology developments such as those in biometrics, body scanners, or indeed even privacy enhancing technologies.

The technology domains identified in bold in Table 4 are discussed in more detail in the following sections. For each domain we give a short description, describe key technologies, discuss how these key technologies in the domain 'fit' for security and/or privacy purposes when used in systems, and attempt to identify societal impact of these technologies in practice when they are used in systems of systems (e.g., for border security). Discussing 'fit' and 'impact' of technologies at the level of technology domains strikes a middle ground between too much detail (i.e. when discussing countless building blocks) and too little detail (i.e. when discussing 'technology' in general).

The discussion for each technology is summarized using a table that shows, in conclusion, the estimated 'fit' of technologies from that domain for security purposes or for privacy purposes, described as 'low', 'average' or 'high', with a brief reasoning as to why this is so.

Security fit:	High/Average/Low – reason
Privacy fit:	High/Average/Low – reason

In addition, the impact that technologies from the domain have when used in practice, e.g. in systems that are used for the EU security missions, is summarized using a similar table, and described as 'negative', 'neutral' or 'positive', also with a brief reasoning as to why this is so.

Security impact:	Positive/Neutral/Negative – reason
Privacy impact:	Positive/Neutral/Negative – reason

Both summaries should be taken with a grain of salt, as most technology domains are complex and the 'average fit' and 'average impact' for technologies from a domain for specific purposes is not possible to determine with quantitative certainty. However, these qualitative estimates, based on technology reports, impact assessments and technology roadmaps, do provide a valuable overview of how the different technology domains impact privacy and security, and how security and privacy is a driving factor in technology development (indicated by the perceived 'fit' of a technology for security or privacy purposes).

4.1.1 Signal & information processing technologies

In practical applications, signal and information processing technologies are closely intertwined with sensor technologies and equipment. Sensor technologies and systems of many kinds provide an ever increasing flow of information about the world, and about the behaviour of persons. Without signal and information technologies the massive amount of data which sensor technologies provide would in many cases be useless, as many sensors provide too much data to be feasibly processed manually. Instead, signal and information technologies automate and improve the processing of information flows, and help identify interesting patterns, classify data to support understanding, and even to increase the value of data by combining it with other data.

Key technologies in this domain include data fusion (integrating multiple sources of data and knowledge into a consistent, accurate and useful representation), automatic data classification (e.g., distinguishing between different kinds of observations), image or audio processing (face

or voice recognition), data mining, text mining, or general information management technologies.

Signal and information technologies are extensively used in digital and physical surveillance scenarios, for example in smart cameras, body scanners or Internet surveillance systems. There is a clear fit for these technologies with security purposes, and especially for surveillance activities. For example, smart camera systems significantly enhance the capabilities of manual camera systems in that facial recognition and other image processing technologies may be used to increase surveillance coverage and reliability, making it possible to identify and track the movements of many individuals simultaneously. Similarly, when combined with digital sensor technologies such as Deep Packet Inspection (DPI), potentially all Internet traffic of individuals could be monitored, analysed for suspicious behaviour, and extremely detailed profiles generated. This would be impossible for more than a few individuals through manual analysis of this data alone. The same is true for monitoring the movements of vehicles, e.g., through the use of automatic number plate recognition.

However, recent developments also show that signal and information processing technologies may, in some cases, also be used to enhance privacy. For example, body scanner systems operated in airport settings to enhance security are often equipped with privacy-enhancing image processing technologies that automatically identify potentially suspicious aspects of an image, and remove the need for human security personnel viewing images of travellers' bodies in high detail. Instead the security personnel get an abstracted 'stick figure' representation of a human body, with an indication where something suspicious may be present. Similarly, image processing technologies in camera surveillance systems are not only used to enhance surveillance capacity, but also to reduce the need for human observers looking at each and every image, therefore also slightly enhancing the privacy of individuals that are viewed by the cameras.

Security fit:	High - automated surveillance and profiling to detect suspicious behaviour
Privacy fit:	Average - privacy preserving automated surveillance

Signal and information technologies are used for several surveillance tasks that follow out of the EU's security missions. Smart camera surveillance is used to detect suspicious behaviour (i.e., potential criminals or terrorists) in airports, city centres and other public and private spaces, and to track vehicles by the use of automated number plate recognition. The scale in which these surveillance systems are applied is increasing rapidly, and the shift to digital technology in camera surveillance brings along with it new concerns with regards to privacy. Digital recording capacities mean that video recordings may be stored, searched, analysed and manipulated with increasing ease. In addition, video recordings can be made available to anyone instantly. Concerns increase that surveillance images may be leaked, manipulated or misused. [22]

[22] Gilbert, Nigel, Anne Anderson, James Backhouse, et al., "Dilemmas of Privacy and Surveillance: Challenges of Technological Change", The Royal Academy of Engineering, London, 2007.

Signal and information technologies are largely invisible to the public, unlike for example video camera systems. As the European Data Protection Supervisor argued at a recent conference:

> *Information communication technologies facilitate the collection, exchange and retention of personal data, often in ways that are not visible to individuals. Even if they are visible, the individual sometimes does not know the nature and scope of what is happening, much less is in control of it.* [23]

Another major societal impact of signal and information technologies lies in the increasing capabilities of Internet surveillance. In the final report of the European Security Research & Innovation Forum several Internet surveillance capabilities are listed as key areas for technological research, we list two such capabilities as examples:

> *Development of new approaches for investigation of the use of the Internet. By monitoring and observing the behaviour of users a search engine for detecting suspicious behaviour patterns should be developed. As an essential element, improved systems for automatic translation can be mentioned*.[24]
>
> *Development of methods and procedures to detect web sites which should be blocked across the EU.*[25]

While this may open new ways in detecting and preventing (organized) crime and planned terrorist attacks, it also gives rise to new concerns with regards to the impact on privacy and civil liberties that operating such systems may have. For example, a system that may be used to block websites across the EU operates on a fine line between EU internal security and government censorship.

From the perspective of law enforcement the increasing amount of personal data that is available on the Internet (e.g., on social network sites or search engines) means that there is a lot of information that is potentially useful for investigations. As a consequence, there exists a strong desire to tap into such information and use it for investigations, collecting evidence and creating profiles, as argued by the assistant European Data Protection Supervisor in a recent talk at a CRID conference.[26]

Security researchers themselves recognize that reconciling the use of digital surveillance technologies with privacy needs more research. Some technological research aims to reduce the privacy impact of signal and information processing technologies used in digital surveillance activities. Such efforts include privacy-preserving data mining, and distributed association-rule mining algorithms that preserve privacy of the individual sites.[27]

---

[23] Buttarelli, Giovanni, "The Surveillance Policy in Europe, Today and Tomorrow", Paper presented at: The Conference for the 30th Anniversary of the CRID, Namur, Belgium, 2010.
[24] European Security Research & Innovation Forum (ESRIF), "ESRIF Final Report", Brussels, 2009.
[25] Buttarelli, Giovanni, "Legal Restrictions – Surveillance and Fundamental Rights", Paper presented at: Conference on New Technical Means of Surveillance and the Protection of Fundamental Rights - Challenges for the European Judiciaries, Vienna, 2009.
[26] Buttarelli, Giovanni, "Welcome address: Fundamental rights at stake", Paper presented at: EDPS Workshop on Video-surveillance with in Community institutions and bodies Brussels, 2009.
[27] INFOSEC Research Council, "Hard Problem List", 2005.

Security impact:	Positive – increased digital and physical surveillance
Privacy impact:	Negative – increased digital and physical surveillance

4.1.2 Artificial intelligence (AI) and decision support

Closely related to (and partially overlapping with) signal and information processing technologies, the domain of artificial intelligence and decision support has a slightly different focus, as implied by the term 'decision support'. AI and decision support aims at structuring, modelling and interpreting information to support decision-making processes, for example during times of crisis.

Key technologies in the AI and decision support domain are expert techniques (allowing digital systems to act as 'experts' on a specific domain), management, modelling and simulation of knowledge, and decision support technologies that support the process of decision making, e.g., by improving the exchange and quick interpretation of critical information.

AI and decision support systems are a good fit for enhancing security at times when decisions involving a lot of different and/or complex sources of information need to be made. This may be a crisis situation (e.g., a natural disaster) or during complex operation (e.g., a large-scale police operation). It is hard, however, to envision a use for enhancing privacy with these technologies.

Security fit:	Average - enhancing security operations (e.g. in times of crisis)
Privacy fit:	Low - not useable for privacy enhancement

Apart from the intended effect - enhanced operations by those responsible for crisis and operations management, and as a result a possible increase in societal safety and security, few societal impacts have been identified in literature for AI and decision support technologies. The exception to this rule lies in the overlap with signal and information processing technologies, e.g., AI technologies used for data mining. However, this has already been discussed in the previous section.

Security impact:	Positive – enhanced decision support in times of crisis
Privacy impact:	Neutral – little impact on privacy

4.1.3 Sensor technologies and equipment

While a lot of research in security revolves around information and communication technologies, another very important technological domain is that of sensor technologies and equipment. In fact, the data that signal and information processing technologies process often originates from sensors and sensor equipment of widely varying kinds.

Key technologies with regards to security in the domain of sensor technology and equipment are cameras, radars, biological and chemical threat detectors, passive IR sensors, terahertz and other subsurface scanners, hyper spectral and multispectral sensors, autonomous small sensors, acoustic sensors, and finally digital 'sensors' such as deep packet inspection. The

wired range of sensor technologies that are currently in active development give an indication of how rapidly the technological eyes, ears, and other senses are expanding in scale and ability.

Sensor technologies of different kinds are of critical importance in security applications, as many approaches to enhance security are based on detecting potential threats, be it humans, dangerous substances, or environmental dangers. Therefore, the domain of sensor technologies has an excellent fit with application in security systems. Surveillance systems such as smart camera systems or Internet monitoring, and threat detection systems such as chemical or biological threat detection in airports, harbours and other domains depend on the availability of dependable sensor systems that provide detailed and accurate data. Visual surveillance systems of different kinds depend on the availability of visual sensors, be it photography, CCTV, imaging scanners, or satellites.[28] The use of sensor technologies is closely tied to signal and information processing technologies, as most sensors provide too much data to be processed manually, and often provide data that is not in a format humans can interpret.

Security fit:	High - essential for detecting security threats
Privacy fit:	Low - not useable for privacy enhancement

While a significant part of the societal impact of security technologies with regards to privacy relates to their "smart" aspects discussed in the signal and information processing technology section, the increasing capabilities of sensors also play a critical role in this.

For video surveillance, improvements in pan-tilt-and-zoom cameras mean that cameras can pan and zoom in on their targets further and further away. Infrared cameras, heat recognition systems and other special cameras can now see in the dark, through walls and through our clothing, as argued by the assistant European Data Protection Supervisor. [29] In addition, cameras are increasingly equipped with audio sensors (microphones), that allow eavesdropping on conversations and detection of suspicious sounds.[30].

The societal impacts of camera surveillance technologies go beyond the cases in which video recordings are actually misused or abused. Indeed, as argued by the assistant EDPS:

> *One can say that being watched sometimes changes the way we behave. Indeed, when watched, most of us censor our speech and our behaviour. In case of widespread or continuous surveillance knowing that our every move and gesture is monitored by the cameras may have a psychological influence as we might need to constantly adjust our behaviour to the expectations of those who are watching us.*[31]

Increasing capacities of sensors to see through clothing covering the human body is used in body scanner systems to enhance security at checkpoints at, for example, airports. The

[28] Gutwirth, Serge, Rocco Bellanova, Michael Friedewald, et al., "Smart Surveillance - State of the Art Report", Deliverable 1, SAPIENT Project, 2012.
[29] Buttarelli, "Welcome address: Fundamental rights at stake", 2009.
[30] Gilbert, et al., 2007.
[31] Buttarelli, "Legal Restrictions – Surveillance and Fundamental Rights", 2009.

increasing use of body scanners has given rise to many privacy concerns, as persons often feel violated in their privacy when security personnel sees them essentially naked using such scanners. The privacy issue has become increasingly visible in the discussions surrounding the use of body scanners, and in research towards improving such scanners the search for more privacy-friendly approaches is intensifying (e.g., as described with regards to millimetre wave scanning technology in)[32] to increase social acceptance of body scanner systems.

Security impact:	Positive – enhanced surveillance and threat detection
Privacy impact:	Negative – reduced privacy of the body and increased surveillance

4.1.4 Social sciences and humanities

The social sciences are somewhat of an exception to the other technological domains discussed here. Instead of developing new technological capabilities the social sciences aim at understanding human behaviour and social processes, including behavioural science, psychology, and cognitive sciences/

Key 'technologies' in the social sciences domain are analysis and modelling of human behaviour at the individual, group and population level, understanding human factors in decision making processes, teams, organizations and cultures.

The social sciences are fit for enhancing security, in that they allow for a better understanding of behaviour and complex social processes that result in security threats or problems, be it flawed decision-making in times of crisis, radicalization of social groups, or failure in identity management systems because of human factors. With regards to privacy, however, the social sciences and the humanities play a more central role in that they help understand the human need for privacy, and what may be involved in protecting privacy.

Security fit:	Average - improving decision making, modelling human behaviour patterns
Privacy fit:	High - essential for understanding privacy needs of humans

The impact of the human sciences are somewhat harder to make explicit compared to the technical sciences, as human sciences rarely result in devices that have an identifiable impact on society. However, the human sciences are the source of privacy researchers that promote the value of privacy, and also contribute to understanding the human need for privacy. In this sense, the impact of the human sciences on society is positive in relation to privacy.

With regard to security the human sciences help understand the social dynamics of groups with high levels of dissatisfaction, and identify stabilizing and destabilizing 'triggers'. Such understanding may form the basis of 'early warning systems' for radicalisation.[33] Such 'early warning systems' are not uncontested with regard to their social impact, however, these systems are often based on having large amounts of data on human behaviour available to them, making them very privacy-sensitive.

[32] European Security Research & Innovation Forum (ESRIF), 2009.
[33] Ibid.

In a different kind of impact, the human sciences help in finding ways to mobilize citizens to behave in an appropriate way for reducing their own risks and - if necessary - contributing to emergency responses, including caring for minorities and weaker individuals and using 'crowd sourcing' approaches to providing critical information in times of crisis.[34] Identity management technologies are critical to both security and privacy and designing an adequate identity management system depends in practice on understanding human behaviour (e.g., with regards to passwords that humans use). Training personnel and creating procedures that enhance privacy protection is also a positive impact of the human sciences with regard to privacy, as illustrated in the following example:

> *An example of an apparently non-malicious human failure was the widely reported case of a hotel in Brighton leaving personal data about guests, including their credit card details, in a skip (reported in the Guardian on January 9th 2006 as 'Risk of ID theft bonanza as thousands of credit card slips found dumped in skip'). These kinds of errors are dangerous but largely avoidable if proper procedures for handling customers' details are put in place.*[35]

Security impact:	Positive – improved models of social dynamics in security
Privacy impact:	Positive – improved understanding of privacy and privacy protection

4.1.5 Information security technologies

Several of the technological domains discussed here are focused on collecting and processing data that provides intelligence that is essential for maintaining security. However, such information itself needs to be protected from unauthorized access or tampering. The information security domain has this protection of information technology itself as its focus.

Information security involves a wide range of building blocks, including many different forms of encryption or cryptography, authentication and authorization technologies, network firewalls, denial-of-service attack protections, session management, digital certification, and monitoring and logging. The information security overlaps partly with the privacy protection domain that is exclusively interested in enhancing privacy, e.g., through the use of anonymisation or zero knowledge proof technologies that may depend on cryptography.

The domain of information security is the source of many technologies that, in principle are a good fit for enhancing both privacy and security when used in systems. Cryptography, for example, forms the basis for securing information through access control, but also forms the basis for enhancing privacy, for example by encrypting personal e-mails so that only the intended recipient may decode and read the message.

Security fit:	High - securing information and information technology is critical to security
Privacy fit:	High - securing personal information is essential for privacy

[34] Ibid.
[35] Gilbert, et al., 2007.

The impact of information security as a technological domain is high, but consists mostly of a reactive impact; information security systems are often created as a response to an information security threat. This may explain a relative lack of studies into the social impact of information security technologies. However, without the protection offered by information security solutions, the increasing dependency of many systems and infrastructures on information technologies would not be possible. Similarly, without information security technologies individuals would be practically defenceless with regard to protecting their privacy in digital environments.

Security impact:	Positive – improved digital security
Privacy impact:	Positive – improved means for digital privacy protection

4.1.6 Navigation and tracking

The navigation and tracking domain is closely related to the sensor technologies and equipment domain, and could be said to be part of that domain. However, since there is such an extensive array of technologies that are used to locate and track objects or persons and their impact is significant separately from the sensor domain, navigation and tracking technologies are discussed as a separate domain here. Navigation and tracking technologies are used to locate, track and follow objects or individuals, and to assist in navigation and direction finding.

Key navigation and tracking technologies are Radio-Frequency Identification (RFID) tags, Global Positioning Systems (GPS), GSM triangulation, radio navigation, automated navigation based on maps, and bar-code based (or matrix barcode based) tracking and tracing.

Navigation and tracking technologies are a good fit for several security-related purposes. First, RFID technologies are often used in access control settings, e.g., in employee cards. Additionally, navigation technologies allow vehicles, ships, and aircraft to navigate safely. Finally, tracking and tracing of objects and important persons using RFID tags, bar-code based tracking, or through other methods, is important in securing supply chains, and keeping track of movements of important (or suspicious) persons and objects (e.g., for preventing theft). Currently no privacy enhancing use for navigation and tracking technologies is known.

Security fit:	High - access control, tracking objects or individuals, safe navigation
Privacy fit:	Low - not useful for enhancing privacy

Navigation and tracking technologies may be used to track the movements of individuals, and technologies from this domain have been the topic of several on-going debates with regard to their (potential) societal impact. One of those technologies is the RFID tag. While persons are not ‘tagged’ themselves (with some exceptions), most individuals carry around a set of RFID tags on their body, be it on clothing or other objects that were bought and that contain an RFID tag for security purposes, or on bank or other cards. The Art. 29 Working Party on Data Protection has expressed serious concerns about the privacy impact of RFID technologies:

> *The ability to surreptitiously collect a variety of data all related to the same person; track individuals as they walk in public places (airports, train stations, stores); enhance profiles through the monitoring of consumer behaviour in stores; read the details of clothes and accessories worn and medicines carried by customers are all examples of uses of RFID technology that give rise to privacy concerns. The problem is aggravated by the fact that, due to its relative low cost, this technology will not only be available to major actors but also to smaller players and individual citizens.*[36]

Another example of such privacy concerns is provided by the Royal Academy of Engineers in their report discussing dilemmas of privacy and surveillance:

> *Information about the journeys made with Oyster cards has been used by the police as a surveillance tool, with the number of requests made by police for Oyster card data increasing. It has been alleged that Oyster card data are used by private investigators to track the movements of spouses suspected of infidelity. Therefore, the Oyster card is not only a means of accessing public transport, but is also a surveillance tool. Although Oyster cards are owned and used voluntarily, the opportunity to opt out of this form of surveillance is taken at a cost. The price differential between journeys paid for by cash and by Oyster card mean that trying to avoid using one is financially punishing, and the options for obtaining and using an unregistered card are limited.*[37]

Another navigation and tracking application is the tracking of the location of mobile devices that connect to the wireless network of telecommunications providers, e.g., through the use of technologies such as GSM, UMTS or LTE technology. As long as a mobile device with such a wireless capability is switched on, the device reveals to the telecommunications provider where they are, with an accuracy of several hundred meters, using triangulation. Telecommunications providers could sell this information to third parties, and police would be interested in accessing this data to support investigations, or to enable surveillance (this already happens in some cases). The potential impact of this type of tracking is especially high since a large number of citizens have such a mobile device, and carry it on their person at all times. The usage and privacy impact of mobile triangulation technology is influenced strongly by the European Data Retention Directive[38], that requires telecommunication providers to store communication and location information for a period of 6 months to 2 years, to allow this data to be available for criminal investigations.

Security impact:	Positive – increased tracking of individuals and surveillance
Privacy impact:	Negative – increased tracking of individuals and surveillance

[36] Article 29 Data Protection Working Party, "Working document on data protection issues related to RFID technology", 10107/05/EN, WP 105, Brussels, 2005.
[37] Gilbert, et al., 2007.
[38] "Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC", *Official Journal of the European Union L 105*, Vol. 49, 15.3.2006, pp. 54-63.

4.1.7 Biometrics

Another special kind of sensor technology, biometrics aims at identifying humans by their characteristics or traits. Key methods (or modalities) used to identify humans in this way include recognition of fingerprints, face, iris, retina, voice, handwriting, signature, palm print recognition, vein pattern recognition, facial thermography, odour recognition, gait recognition, keystroke dynamics, and DNA. Several different forms of biometrics may be combined to enhance their reliability.

Biometrics are of high importance and an excellent fit for security purposes, since they could potentially offer a form of identification that is extremely difficult to fool. Indeed, biometrics are already used in many places in the EU, e.g., in facilitating cross-border checks. For enhancing privacy, however, biometrics do not appear to be useful, except for rare cases in which information could be secured using biometric technologies.

Security fit:	High - identification and access control
Privacy fit:	Low - not useful for enhancing privacy

Biometric technologies have been the centre of heated debate about their societal impact, especially with regard to privacy. Citizens' rights organizations oppose the use of biometrics out of concern for privacy and civil liberties. One concern is that the use of biometrics in ID cards (as is currently the case in several EU Member States) requires that biometric characteristics of all citizens be recorded and stored, which is a shift from the situation in which most EU states only would record fingerprints of criminals.[39]

Concerns about the societal impact of biometrics are further strengthened as biometric technologies rapidly improve in accuracy and ability. For example, new forms of biometrics are being investigated such as using an individual's baseline brainwave pattern from an electroencephalogram (EEG) for identification, or footprint recognition, as well as recognition based on the shape and physiological structure of the tongue.[40]

Security impact:	Positive – enhanced access control and border checks
Privacy impact:	Negative – increased and improved identification, also in surveillance

4.1.8 Integrated platforms

The integrated platforms domain stands out from the others discussed here in that it aims at developing integrated systems (platforms), and not necessarily separate building blocks. Integrated platforms are related to several other domains, most notably sensors because these platforms may be used as a platform upon which to mount sensors. Some key technologies in the integrated platforms domain are unmanned aerial vehicles (UAVs), unmanned sea or land vehicles, lighter than air platforms, and surveillance and navigation satellites.

[39] Hayes, Ben, "Arming Big Brother: The EU's Security Research Programme", TNI Briefing Series No. 2006/1, Transnational Institute; Statewatch, Amsterdam, 2006.
[40] The Irish Council for Bioethics, "Biometrics: Enhancing Security or Invading Privacy?", Dublin, 2009.

Integrated platforms are a good fit for several varied security purposes, ranging from police surveillance through the use of UAVs with cameras, [41] to satellites monitoring for environmental security or enabling navigation capabilities. For privacy, however, no uses were found for such platform.

Security fit:	Average - surveillance from the sky
Privacy fit:	Low - not useful for enhancing privacy

Integrated platforms have been the focus of some discussion about their impact, especially when they are armed. Attacks by USA-controlled 'drones' in Afghanistan and Pakistan have been contested from a human rights perspective for some time. From the viewpoint of privacy, however, only few issues have been raised so far. UAVs for peacetime security may be used to perform police or border surveillance from the sky, potentially violating the privacy of persons expecting to be safe from surveillance e.g., in their garden.[42]

Security impact:	Positive – enhanced surveillance
Privacy impact:	Negative – surveillance from the sky violating privacy of the home

4.1.9 Energy generation, storage and distribution

While much research in the domain of energy generation, storage and distribution is not explicitly aimed at security, it involves many security-related challenges, either by ensuring energy supply security. This is a research domain that also has a focus on infrastructural issues, e.g., (in)stability of the electrical power grid. Key technologies that are part of this field include electrical generators, electrical batteries, energy distribution, and security of smart grids.

The security of the energy supply is extremely important to societal security, and as such research in the stability, resilience and security of the energy grids is a good fit with infrastructural security aims. For privacy no uses of such technologies are known.

Security fit:	Average - ensuring security of critical energy infrastructure
Privacy fit:	Low - not useful for enhancing privacy

Research into the security of the energy infrastructure is responsive to an ever increasing dependency on this infrastructure, and new vulnerabilities introduced by recent developments in technologies like smart grids. Some Member State governments have recognized that smart grids introduce an increased dependency on the security of information technologies in the energy infrastructure, as well as new risks. ENISA investigated several National Cyber Security Strategies, and concluded that:

> *The main points covered by a typical National Cyber Security Strategy are usually: […] To identify critical information infrastructures (CIIs) including key assets, services and*

[41] Gutwirth, et al., 2012.
[42] Finn, Rachel L. and David Wright, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", *Computer Law & Security Review*, Vol. 28, No. 2, 2012, pp. 184-194.

> *interdependencies. To develop or improve preparedness, response and recovery plans and measures for protecting such CIIs (e.g. national contingency plans, cyber exercises, and situation awareness).*[43]

In addition to the security concerns surrounding the energy infrastructure, recent developments in smart grids also give rise to privacy concerns. The source of these concerns is that part of the smart grids infrastructure is extended into the homes of families in the form of a smart meter that digitally records energy consumption over time, and transmits this information periodically to the energy supplier. Privacy concerns arise because this energy consumption information could tell many things about an individual's behaviour, e.g., whether he or she is home at certain times or what kinds of appliances are being used at what times.

Security impact:	Positive – enhanced security of critical infrastructure
Privacy impact:	Negative – smart metering may violate privacy of the home

4.1.10 Privacy protection

A final technological domain that partially overlaps with the information security domain is research that aims explicitly at enhancing privacy, usually focusing on information privacy. Although this domain consists in part of researchers that work in the information security domain, a growing group of researchers focuses explicitly on privacy protection technologies.

Key technologies that are part of this domain are anonymisation of data, zero knowledge proofs (proof of a claim without requiring identification of the person making the claim), mix networks and onion routing (untraceable internet communication), privacy by design (privacy protective design approaches), and tools for providing control and transparency on the handling of personal information to users.

Unsurprisingly, this field of research has an excellent fit for the purpose of enhancing privacy. However, technologies being developed here are sometimes also useful for security purposes, for example zero knowledge proofs may be theoretically used for access control while preserving an individual's privacy.

Security fit:	Average - several technologies aim at securing communication
Privacy fit:	High - these are key technologies used to enhance privacy of individuals

Providing individuals with technologies to protect their information is one of the Information Security Hard Problems identified by the IRC Research Council:

> *Historically, governments have cited compelling national security needs for seeking to violate privacy. An example of such arguments is that security is most effective when based on actual and timely information that can be attained only through pervasive*

[43] ENISA (European Network and Information Security Agency), "National Cyber Security Strategies - Setting the Course for National Efforts to Strengthen Security in Cyberspace", May, Heraklion, Crete, 2012.

> *monitoring. In contrast, individuals and corporations cannot function in a modern society unless they have means to protect certain types of information. Protecting digital information relies on the use of encryption, steganography, sanitization, or anonymizers when sending electronic communications. Paradoxically, the use of these protection techniques can be viewed as a significant challenge to national security organizations responsible for identifying potential threats and to pre-empting planned attacks. This apparent contradiction may not be amenable to a resolution. Even so, various possible approaches appear promising.*[44]

One of the conclusions drawn here is that the use of privacy protection technologies has a perceived negative impact on societal security, as increasing use of privacy enhancing technologies makes several kinds of surveillance more difficult, and detecting suspicious behaviour and threats harder. This is especially true for digital surveillance, for example on the internet. Privacy enhancing tools such as onion routing and the Tor network (making it difficult or impossible to connect sender and receiver of digital communications) in some cases are identified as a security risk for organizations.[45]

Security impact:	Negative – hinders (internet) surveillance and criminal investigations
Privacy impact:	Positive – protects the privacy of individuals and groups

4.2 RELATING TECHNOLOGIES USING KEYWORDS

Part of the data mining approach taking during data collection for the analysis was an examination of what privacy and security related keywords are typically used together in research proposals listed on CORDIS. For example, researchers were interested in whether cryptography is typically associated with privacy or with security, or whether the use of surveillance as a term increased after significant historical events such as large terrorist attacks.

While the original attempt at the data mining methodology used a much larger list of keywords (e.g., including the building blocks listed in Table 4), most of these keywords were not used at all in the high-level project objective descriptions (see also section 2.3 on the approach). In consequence, researchers manually-selected a list of keywords that did occur, and reviewed them for relevance. The result of a data mining effort on these keywords is shown in Figure 1 on the next page.

[44] INFOSEC Research Council, 2005.
[45] "Check Point 2013 Annual Security Report", Check Point Software Technologies Ltd., Tel Aviv; San Carlos, Cal., 2013.

	# times keyword used	privacy	security	surveillance	privacy enhancing technolog	anonymisation	privacy by design	zero-knowledge proof	number plate	crypto	access control	smart grid	infrastructure	rfid	gps	data mining	cctv	video	camera	biometric	fingerprint	iris
privacy	270	100%	63%	6%	2%	0%	1%	0%	0%	12%	4%	0%	33%	4%	2%	4%	1%	6%	2%	6%	3%	1%
security	1468	12%	100%	5%	0%	0%	0%	0%	0%	5%	2%	0%	21%	1%	1%	2%	1%	4%	2%	2%	1%	1%
surveillance	101	16%	67%	100%	0%	0%	2%	0%	1%	0%	2%	2%	27%	2%	4%	0%	5%	28%	21%	2%	0%	2%
privacy enhancing technolog	5	100%	100%	0%	100%	0%	0%	0%	0%	60%	0%	0%	20%	0%	0%	20%	0%	0%	0%	20%	20%	0%
anonymisation	1	100%	0%	0%	0%	100%	0%	0%	0%	0%	100%	0%	100%	0%	0%	0%	0%	0%	0%	0%	0%	0%
privacy by design	2	100%	50%	100%	0%	0%	100%	0%	0%	0%	0%	0%	0%	50%	0%	0%	50%	0%	0%	0%	0%	0%
zero-knowledge proof	1	100%	100%	0%	0%	0%	0%	100%	0%	100%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
number plate	1	100%	0%	100%	0%	0%	0%	0%	100%	0%	100%	0%	0%	0%	0%	0%	0%	100%	0%	0%	0%	0%
crypto	80	40%	88%	0%	4%	0%	0%	1%	0%	100%	6%	0%	21%	3%	0%	4%	0%	1%	3%	9%	5%	1%
access control	30	40%	77%	7%	0%	3%	0%	0%	3%	17%	100%	0%	33%	0%	3%	0%	3%	13%	10%	20%	7%	10%
smart grid	10	10%	70%	20%	0%	0%	0%	0%	0%	0%	0%	100%	60%	0%	0%	10%	0%	0%	10%	0%	0%	0%
infrastructure	416	22%	75%	6%	0%	0%	0%	0%	0%	4%	2%	1%	100%	1%	0%	3%	1%	3%	2%	2%	1%	0%
rfid	21	52%	81%	10%	0%	0%	5%	0%	0%	10%	0%	0%	24%	100%	0%	5%	10%	0%	0%	10%	0%	0%
gps	18	28%	56%	22%	0%	0%	0%	0%	0%	0%	6%	0%	11%	0%	100%	6%	0%	6%	0%	0%	0%	0%
data mining	30	33%	77%	0%	3%	0%	0%	0%	0%	10%	0%	3%	37%	3%	3%	100%	0%	0%	0%	0%	0%	0%
cctv	10	20%	80%	50%	0%	0%	10%	0%	0%	0%	10%	0%	30%	20%	0%	0%	100%	50%	40%	10%	0%	0%
video	79	20%	76%	35%	0%	0%	0%	0%	1%	1%	5%	0%	18%	0%	1%	0%	6%	100%	25%	3%	1%	0%
camera	47	11%	77%	45%	0%	0%	0%	0%	0%	4%	6%	2%	19%	0%	0%	0%	9%	43%	100%	4%	2%	4%
biometric	42	40%	86%	5%	2%	0%	0%	0%	0%	17%	14%	0%	24%	5%	0%	0%	2%	5%	5%	100%	24%	12%
fingerprint	19	37%	95%	0%	5%	0%	0%	0%	0%	21%	11%	0%	21%	0%	0%	0%	0%	5%	5%	53%	100%	21%
iris	10	30%	80%	20%	0%	0%	0%	0%	0%	10%	30%	0%	10%	0%	0%	0%	0%	0%	20%	50%	40%	100%

Figure 1 - keyword relation analysis: red indicates a strong relation, blue indicates no relation. Read this as follows, e.g. for the privacy(1st row)/security(2nd column) cell: in 63% of the CORDIS objective descriptions where 'privacy' was mentioned, 'security' was also mentioned. Vice versa, in 12% of the descriptions where "security" was mentioned, the word "privacy" was also mentioned. Note that the table is not symmetric, e.g. privacy is mentioned less often in documents that mention security than the other way around.

While the outcomes of this data mining effort visualized in Figure 1did not result in ground-breaking discoveries, it did result in some interesting insights. The "privacy" keyword was relatively frequently combined with cryptography, surveillance, infrastructure, video, and biometrics. The "security" keyword, on the other hand, was relatively frequently combined with surveillance, cryptography, and infrastructure. After manually reviewing some of the documents in which the keywords were used together to determine the correct interpretation of these results, we draw some conclusions:

- cryptography is an important enabler for both security and privacy solutions;
- surveillance technologies are used as an important enabler to enhance security, but raise privacy concern;
- video surveillance and biometrics have been significant concerns in privacy-oriented research over the past decade; and
- security of critical infrastructure is an important issue in security-related research.

4.3 SYSTEMS OF SYSTEMS

As defined in chapter 3, systems of systems are a combination of different systems for an overarching purpose. Systems of systems may be defined at different levels, e.g. a corporate access control security system of systems or a national border surveillance system of systems. In this discussion the term systems of systems is used to identify large EU-wide systems that aim at enhancing one of the main security needs of the EU. A number of different high-level security needs may be identified, as is presented in Figure 2.

Figure 2 – The EU's main security missions[46]

In another and more detailed subdivision of security objectives of the EU, the European Commission identifies five main objectives for the EU internal security strategy:

- *objective 1 — Disrupt international crime networks;*
- *objective 2 — Prevent terrorism and address radicalisation and recruitment;*
- *objective 3 — Raise levels of security for citizens and businesses in cyberspace;*

[46] The EU's four main security missions are listed on the EC's Security research and industry website: http://ec.europa.eu/enterprise/policies/security/missions/index_en.htm

- *objective 4 — Strengthen security through border management; and*
- *objective 5 — Increase Europe's resilience to crises and disasters*[47]

For each of these objectives, different technologies and systems are a good 'fit', and are typically used. While these missions are very large in scale, and very complex, and therefore many different technologies are used, we highlight out some key technologies which we have discussed in section 4.1:

- **Disrupt international crime networks:** AI and decision support, Internet surveillance, privacy protection.
- **Prevent terrorism and address radicalisation and recruitment:** Internet surveillance, data fusion, data mining, human behaviour modelling, modelling group radicalization, smart grids security.
- **Raise levels of security for citizens and businesses in cyberspace:** information security technologies, human sciences, privacy protection.
- **Strengthen security through border management:** biometrics, body scanners**,** integrated (aerial) platforms for border surveillance, automatic number plate recognition.
- **Increase Europe's resilience to crises and disasters:** AI and decision support, satellite technology for environmental monitoring.

4.4 EUROPEAN RESEARCH

One of the key questions behind the data mining effort was whether there was a noticeable shift in attention to privacy as a research topic compared to security over time. To this end, researchers counted the relative usage of the keyword 'privacy' and 'security'. Note that the corpus over which this analysis was performed consisted only of those CORDIS projects that had 'privacy' OR 'security' in their objective descriptions already. The result of this analysis is visualized in Figure 3.

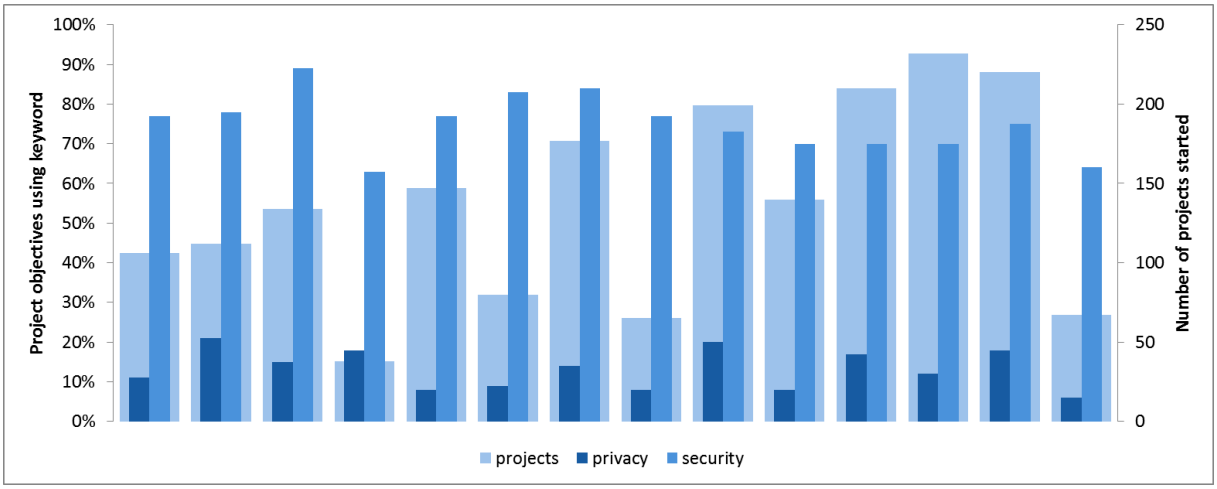

Figure 3 – relative keyword usage over time: percentage of CORDIS objective descriptions in which keyword is used

The remarkable thing about this outcome is not a significant shift in the attention towards privacy or security, but rather that attention towards both privacy and security remains

[47] European Commission, "The EU Internal Security Strategy in Action: Five steps towards a more secure Europe", COM(2010) 673 final., Brussels, 2010.

balanced over time, and does not show a noticeable shift on the long run. Also noticeable is that privacy has been a point of attention in research projects in all the framework programmes.

A further analysis of the research objective corpus was performed in a similar way, only counting the usage of keywords relating to internal security missions of the EU: critical infrastructures, terrorism and organized crime, security in times of crisis, and border security. The results of this data mining efforts are visualized in Figure 4 below.

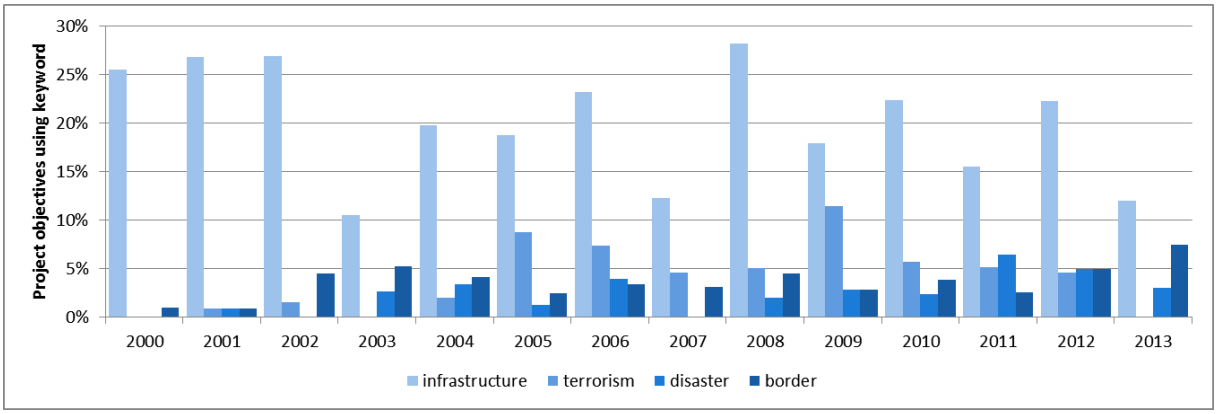

Figure 4 - relative keyword usage over time: percentage of CORDIS objective descriptions in which keyword is used

The attention to infrastructure is relatively high compared to the other topics. A possible explanation for this difference is that the word 'infrastructure' is used in other meanings than that of critical infrastructures, e.g., a 'privacy-friendly identity management infrastructure', which may inflate this usage. For terrorism, crisis, and border security this is less likely.

One noticeable shift is visible in the use of the keywords related to terrorism and organized crime security missions from 2004 and onwards. A plausible explanation for this may be that this is a (delayed) response to the 9/11 attacks and other attacks around this time period. Recently the use of 'crisis' as a keyword increased significantly, which may have to do more with the economic crisis that started in 2008 rather than with a shift in attention towards disaster management. Other than a clear shift in attention towards research that relates to the security mission of fighting terrorism and organized crime, few significant shifts in research focus can be derived from this data mining effort.[48]

The final data-mining effort explored the usage of terms relating to capabilities that are key to many security applications and that strongly relate to privacy issues: 'detection', 'identification', and 'surveillance'. The results of this effort are visualized in Figure 5.

[48] In the final deliverable for this work package, some improved data mining efforts may be presented, e.g. based on an analysis of a series of full-text research reports. The feasibility and usefulness of such efforts is being examined.

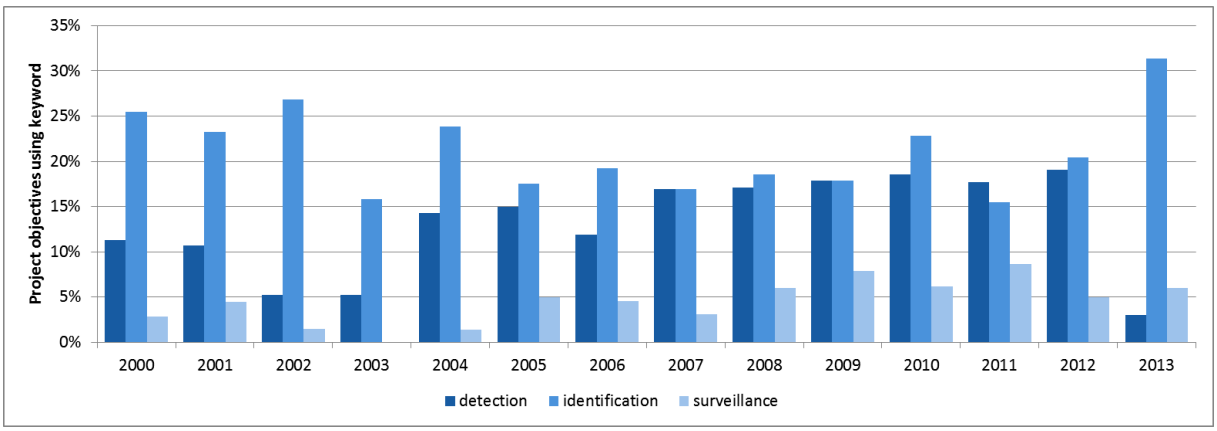

Figure 5 - relative keyword usage over time: percentage of CORDIS objective descriptions in which keyword is used

In this result, a number of things are noticeable. First of all, there is a significant increase in the use of the keyword 'detection' from 2004 onwards (particularly in project descriptions that also use the word 'security' or 'privacy'). In addition, the use of the word 'surveillance' appears to increase after 2004. In the use of the keyword 'identification', no clear trend is visible.

To get a clearer picture of how security and privacy related research developed over time in the EU framework programmes, the next two pages give an overview of a selection of security and privacy related research projects funded by the European Union over the years. The overview was generated based on the corpus, and each project was manually selected for relevance and privacy or security focus.

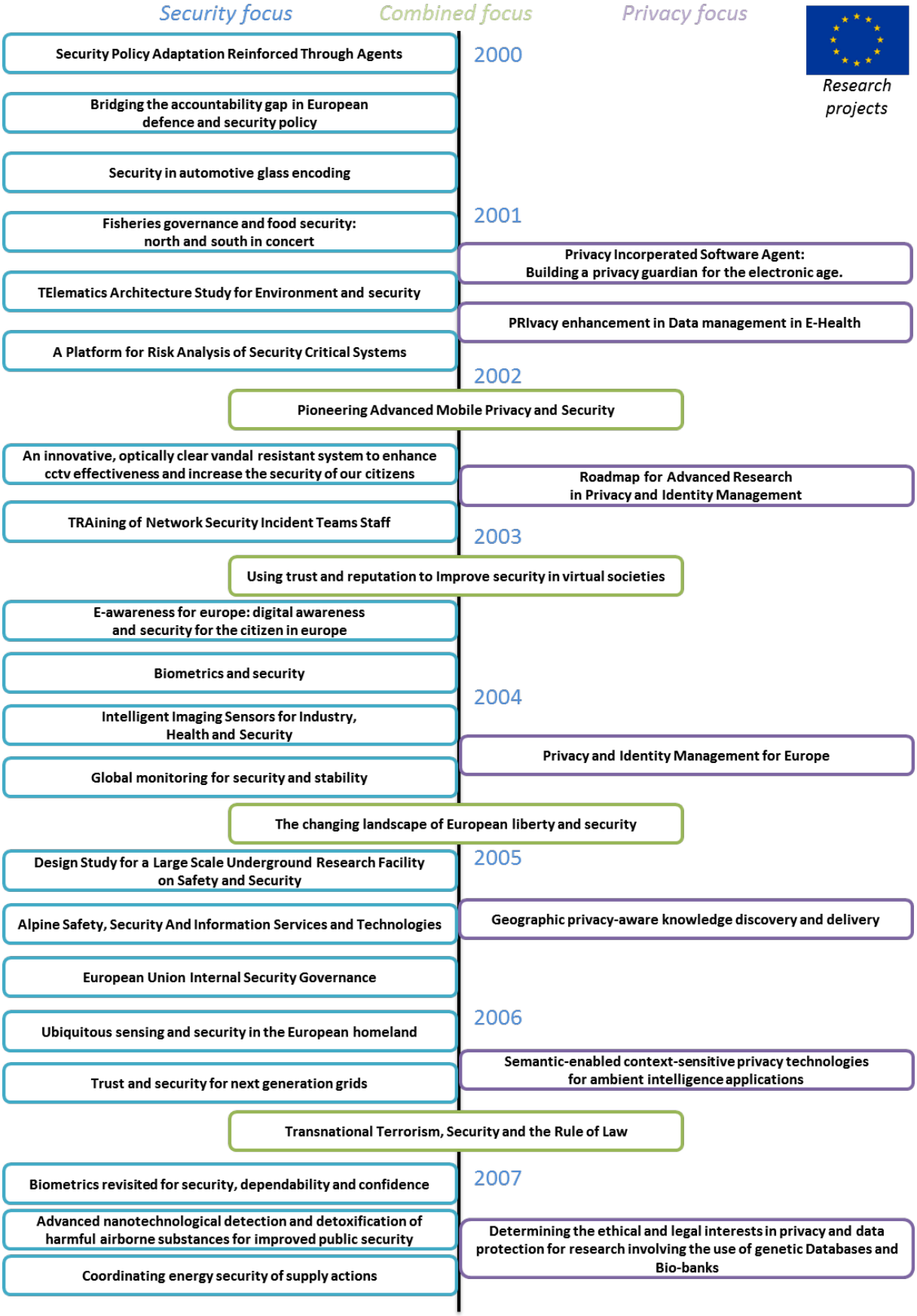

Figure 6 – research project focus over time (based on data mining of CORDIS project objectives)

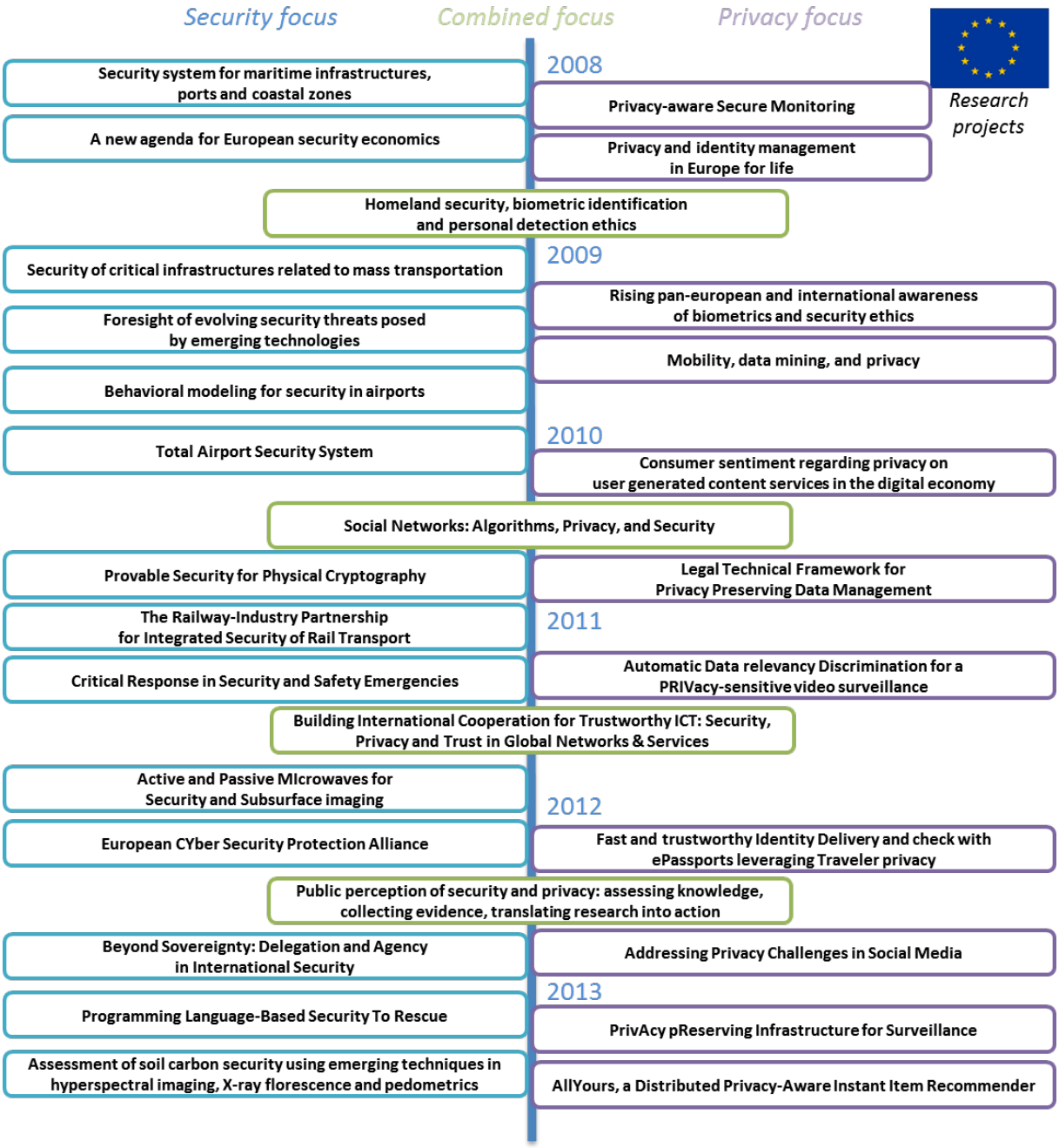

Figure 6 (continued) – research project focus over time (based on data mining of CORDIS project objectives)

This overview shows a wide variety of security projects, which corresponds to the many meanings encompassed within security as a concept. A lot of 'security'-related research does

not appear to affect privacy directly, e.g., alpine safety, food security, and automotive glass security. Other security-related research does appear to affect privacy, e.g., behavioural modelling for airport security, biometrics, and subsurface imaging. Several research projects appear to treat privacy and security as equal values, e.g., assessing public perception, liberty and security, and advanced mobile security and privacy.

Several projects demonstrate an intention to overcome a perceived tension between security and privacy objectives. Examples are privacy-aware secure monitoring, privacy-sensitive video surveillance, and personal detection ethics. The importance of the human sciences in identifying and overcoming privacy challenges is visible in several projects which have a focus both on privacy and security, and aim to understand the dynamics of security and privacy, the ethical issues involved in security policy, and public perception of security and privacy.

4.5 ANALYSIS

The assessment of technology domains in section 4.1 yielded a global 'fit for purpose' estimate of technologies in these domains for security or privacy purposes. Also, a preliminary assessment of the impact of technologies in these domains on privacy and security capabilities in practice was given. These assessments are summarized for the domains in Table 5 below:

	Fit for purpose		**Impact in practice**	
Technology domain	**Security**	**Privacy**	**Security**	**Privacy**
Signal and information processing tech.	High	Average	Positive	Negative
Artificial intelligence and decision support	Average	Low	Positive	Neutral
Sensor equipment and Sensor technologies	High	Low	Positive	Negative
Human sciences	Average	High	Positive	Positive
Information security technologies	High	High	Positive	Positive
Navigation and tracking	High	Low	Positive	Negative
Biometrics	High	Low	Positive	Negative
Integrated platforms	Average	Low	Positive	Negative
Energy generation, storage and distribution	Average	Low	Positive	Negative
Privacy protection	Average	High	Negative	Positive

Table 5 – overview of technology domains assessment on fit for purpose and impact

It is important to note that this is a preliminary overview; the listed impacts on security and privacy of technology domains an early assessment based on existing technology roadmaps and reports. Nearly all technological domains that were examined yield technologies are expected to have a positive impact on security when used in systems. In fact, for most of these domains enhancing security-related capabilities are important arguments for investing in technology research and development. A positive impact on privacy is only visible for technologies from three domains: the human sciences, information security, and privacy protection.

Two technology domains stand out from the rest in this table: information security and privacy protection. Information security is a unique field of research in that it yields technologies that are a good fit for both security and privacy purposes. The overlap between security and privacy that is visible here is part of the protection of personal data.

An overview of fit for use and impact on privacy and security of technology domains is a useful tool for policy makers. It makes it possible to get an early estimate what the effects of investments in different research domains may be with regards to security and privacy capabilities, and what the impact ultimately may be in society.

While important for the overview, a high-level assessment such as this lacks in nuance needed for a deeper understanding of the issues involved. However, in task 2.2 of the PRISMS project, we will assess a selection of building blocks and systems from a socio-technical perspective, and in much more detail.

4.5.1 Fit for Purpose and Impact in Practice

In Table 5 there are similarities between the fit for purpose of technologies from a domain and their assessed impact in practice. For example, sensor equipment and technologies have a high fit with security purposes and a low fit for privacy purposes. These technologies also have a positive impact on security and a negative impact on privacy (based on this preliminary assessment) when applied in practice. Technologies with a high fit for a certain purpose may be assumed to also have a positive impact in achieving this purpose when used in practice. This is not always true the other way around, however: technologies with a low fit for a certain purpose do not necessarily negatively impact achieving this purpose in practice.

Technology reports and roadmaps typically focus on the fit for purpose of building blocks. Certain overarching goals need to be achieved (e.g. the EU security missions), and technology development is steered towards developing capabilities that will make achieving the goal, in theory, possible. Impact assessments, and to some extent policy documents that were studied usually focus on the impact in practice of technology systems, and less on their fit for purpose. This is visualized in *Figure 7* below:

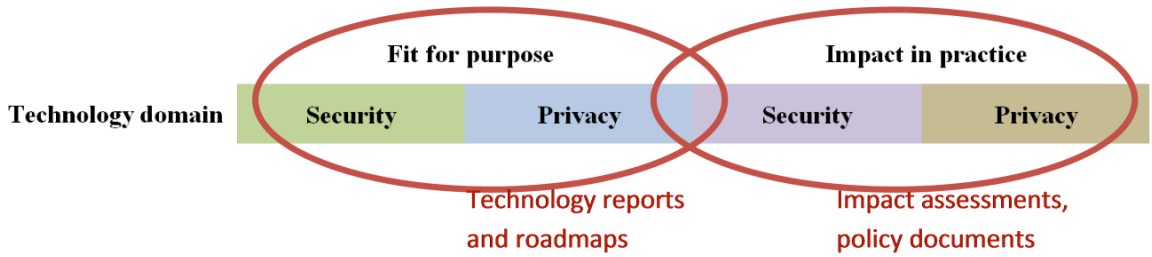

Figure 7 – focus on fit for purpose or impact in practice

This difference in focus becomes important when discussing the trade-off that exists in technological development between security and privacy. This trade-off is not visible in the fit of technologies for privacy or security purposes but it does become an issue when technologies are used in practice and have an impact on society.

A focus on the fit for purpose of technologies in technology reports and roadmaps does not imply that there is no attention whatsoever to the (societal) impact of technologies in these documents. In many security technology-related reports and roadmaps some attention is given to societal issues related to security research, technology, and industrial activity, especially where it relates to privacy. For example, the ESRAB 2006 report states:

> *Respect of privacy and civil liberties should be the programme's guiding principle. In this sense research and development projects should take into account the mutual dependency triangle of technology, organisational dynamics and human impact.*[49]

This indicates an awareness of that the use of security technologies may have a negative impact on privacy and civil liberties. One reason for the attention towards the privacy and other societal impacts of security technologies is that these issues play a role in the social acceptance and legal compliance of security technologies and security industry activities. This social acceptance is a general challenge across different industrial sectors, but the security industrial sector is special in a number of ways. As noted in the 2012 EC Security Industrial Policy, security technologies may 'directly or indirectly concern fundamental rights, such as the rights for respect for private and family life, protection of personal data, privacy or human dignity.'[50] Another factor that increases the social impact of security technologies is that in most cases citizens do not a real choice to avoid such technologies when they are implemented; for example if someone wishes to travel by plane the security measures in airports cannot be avoided. Finally, the impact of security technologies is increased by the fact that they are typically highly visible, e.g., everyone going into an airport is directly confronted with several highly security measures such as several security checkpoints.[51]

4.5.2 A Trade-off

One issue that is clearly visible in Table 5 is a trade-off between security and privacy that is inherent in technology development and use. Increased investments in technologies that have a positive impact on security tend to simultaneously have a negative impact on privacy. Some notable exceptions exist, however: the fields of information security and human sciences do not show such a trade-off. A possible explanation may be the lack of nuance in this assessment: perhaps some technologies in these domains may have negative impacts, but overall the effect is perceived to be positive for both privacy and security in most reports, assessments and roadmaps.

A trade-off between privacy and security is also visible with regards to privacy protection technologies, especially when it comes to security by internet surveillance. Technologies

[49] ESRAB (European Security Research Advisory Board), 2006.
[50] European Commission, "Security Industrial Policy: Action Plan for an Innovative and Competitive Security Industry", COM(2012) 417 final Brussels, 2012.
[51] Ibid.

specifically developed to enhance anonymity and to secure communications (showing an overlap with the information security domain) are perceived by some reports as having a negative impact on security through surveillance.

With regard to potential impacts on privacy, a number of highly connected technological domains stand out from the rest: sensor technologies and equipment, biometrics, and signal and information processing technologies. The combination of building blocks from these domains leads to detection, identification, and surveillance systems that have an especially severe impact on privacy, e.g., systems such as body scanners, biometric identification, and smart camera surveillance. The trade-off between security and privacy is most pronounced with regards to these technologies that enhance surveillance capabilities. These capabilities are currently rapidly increasing due to a culmination of different technological developments that are a good fit for surveillance purposes, for example improved cameras and other sensors, airborne and other platforms for mounting these cameras and sensors, and a massively increased capacity for processing and interpreting surveillance data. This is both true for traditional camera surveillance, and for relatively new forms of surveillance such as internet surveillance.

Figure 5 confirms this trend: the use of the keyword 'surveillance' in CORDIS research objective descriptions has significantly increased in the past decade. On the internet some privacy protection technologies (e.g. onion routing networks, encryption) provide a counterweight to internet surveillance to some extent. This technological counterweight is absent, however, for surveillance in physical private and public spaces.

The preliminary conclusion of this analysis is that there is a clear trade-off between security and privacy in technology development and use in practice. In other work packages and tasks of the PRISMS project, we will assess this trade-off in more detail and with more nuance. Task 2.2 builds on this assessment by analysing a selection of technologies as socio-technical systems, to learn how perceptions of privacy and security and the trade-off between them are embedded in new and current security systems.

4.6 DRIVERS AND BARRIERS

Technology development is subject to factors that drive it or hinder it, influencing how the trade-off between security and privacy turns out. We performed a preliminary analysis of the drivers and barriers that respectively drive security and privacy technological developments, or act as barriers to these developments. The drivers and barriers outlined here are based on a literature study of policy documents, technology roadmaps, foresight studies and impact assessments. Most drivers and barriers that were identified apply to both security and privacy technology developments, although to a varying extent.

4.6.1 Driver: technology and industry push

The 'military industrial complex' has become a reality by the farewell speech of Dwight Eisenhower in 1961, ending his presidential career. Eisenhower first stipulates the emergence of the military industrial complex, new in the American experience, and in his view the result of the changing approach to arms and armaments after the three large wars in which the United Stated have been involved (the first and second world war, the Korean war). Eisenhower states:

> *Now this conjunction of an immense military establishment and a large arms industry is new in the American experience. The total influence -- economic, political, even spiritual -- is felt in every city, every Statehouse, every office of the Federal government… [W]e must not fail to comprehend its grave implications. In the councils*

> *of government, we must guard against the acquisition of unwarranted influence, whether sought or unsought, by the military-industrial complex. The potential for the disastrous rise of misplaced power exists and will persist. We must never let the weight of this combination endanger our liberties or democratic processes. We should take nothing for granted. Only an alert and knowledgeable citizenry can compel the proper meshing of the huge industrial and military machinery of defence with our peaceful methods and goals, so that security and liberty may prosper together.*

This quotation is presented at length, since Eisenhower both addresses the emergence of a complex consisting of industries at arm's length of military decision makers and the role and responsibilities of "alert and knowledgeable citizenry" in order that "security and liberty may prosper together". Several authors indicate that this military-industrial complex meanwhile has experienced a transition into the direction of a security-industrial complex, since the revenues for military undertakings are under pressure. While a security-industrial complex may be identifiable in the current European context, a 'privacy-industrial complex' is more difficult to distinguish. Furthermore, in so far it is present, it may partially overlap with the security-industrial complex, as companies offering security-enhancing solution may also offer privacy-enhancing solutions, or indeed the very same solutions may be used to enhance both security and privacy (e.g., in the case of encryption of communications or sensitive data).

The security-industrial complex is significant in Europe, and is developing at a rapid pace. The pace of these developments to a large extent based on increasing demand. [52] However, a vested industry also has a significant interest in maintaining and increasing demand for its products and services. Industry, and to some extent research institutions, that are involved in researching and developing technologies for security and privacy provide a 'technology push', or solutions in search of a problem.

Due to the size of the security industrial complex compared to a 'privacy industrial complex', the effect of this 'technology push' may be expected to be much more pronounced for security technologies than for privacy technologies. Companies developing privacy protection solutions currently operate mostly in niche markets, and provide a 'technology push' to a lesser extent.

4.6.2 Driver: events with high societal impact

In Figure 4 we saw that the use of the keywords related to terrorism and organized crime in CORDIS project objective descriptions increased markedly from 2004 and onwards. A possible explanation for this is that this is a delayed response to a number of high-profile attacks on the EU and its allies, resulting in an increased attention in fighting terrorism and organized crime. These attacks include the September 11 airplane hijack and subsequent attack in 2001 in New York and Washington, the July 7 2005 suicide bombings of the public transport system in London, and the March 11 2004 Madrid train bombings. All these events have had a high impact on the perception of security (or the lack thereof) of citizens in the EU, and as a consequence an increased call for security and protection against such terrorist attacks, even at the cost of losing privacy.

[52] Wright, David, Iván Székely, Michael Friedewald, et al., "Surveillance, fighting crime and violence", IRISS Deliverable 1.1, 2012.

While assessing this interplay between security and privacy as a consequence of high-profile societal events is outside the scope off this deliverable, we identify these events as a possible driver of primarily development of security technologies. To a much lesser extent some high-profile privacy-related incidents (e.g. leaks of large amounts of personal data) may drive the development of privacy protection technologies.[53]

4.6.3 Driver: national and EU-level policy and regulation

Although national and EU-level regulation tend to be reactive and sometimes fragmented, legislation does act as a driver for organizations to implement certain privacy and security protections, to be compliant with the law.[54] The strength of this driver depends amongst other things on the presence and actions of a supervising authority (e.g. data protection supervisor), and how well organizations understand what they have to do to be compliant, which is an issue especially with regards to privacy.

A special case of this driver is the charter of fundamental rights as argued in the 2010 EU Internal Security Strategy:

> *People in Europe expect to live in security and to enjoy their freedoms: security is in itself a basic right. The values and principles established in the Treaties of the Union and set out in the Charter of Fundamental Rights have inspired the EU's Internal Security Strategy: justice, freedom and security policies which are mutually reinforcing whilst respecting fundamental rights, international protection, the rule of law and privacy […], transparency and accountability in security policies, so that they can be easily understood by citizens, and take account of their concerns and opinions.*[55]

4.6.4 Driver: citizen demand for security and privacy

Another driver is related to some of the drivers we already mentioned: citizens demand a certain level of security and privacy, and as a consequence a market for products may arise, or governments may setup regulations. Citizen demand plays a role in the application of some surveillance technologies, such as CCTV cameras. A perception of being insecure, e.g. being threatened by crime or violence in city centres, may increase the demand for technologies that are perceived to enhance security, such as surveillance systems. This does not necessarily mean that these solutions are effective in enhancing security. [56]

With regards to privacy the same driver applies: citizens demand a certain level of privacy, for example while using internet services, and as a consequence new technologies get developed that fill in this demand. An example is the Do Not Track technology used in web browsers.

---

[53] van Lieshout, Marc, Linda Kool, Gabriela Bodea, et al., "Stimulerende En Remmende Factoren Van Privacy by Design in Nederland", TNO, Delft, 2012.
[54] European Commission, "Security Industrial Policy: Action Plan for an Innovative and Competitive Security Industry", 2012; van Lieshout, et al., 2012.
[55] European Commission, "The EU Internal Security Strategy in Action: Five steps towards a more secure Europe", 2010.
[56] Wright, et al., 2012.

4.6.5 Barrier: security and privacy are often not unique selling points

Although citizen needs for security and privacy may increase demand for certain technologies that aim to enhance security or privacy, for many services and products security and privacy is not the primary focus, but rather a side issue. For example, for most of the transport sector, transporting goods and passengers is the primary activity, and security and privacy, while important, both do not act as positive selling features that companies advertise.[57] The same is true with regards to privacy: few companies see privacy as a unique selling point that allows them to sell products better or to compete better. Customers do currently not seem to find privacy a distinguishing feature of services, and are not overly willing to pay for enhanced privacy protection.[58]

Increasing awareness of the importance of privacy and security with customers may possibly change this barrier into a driver, however. In the EU Security Industrial Policy, aspects such as privacy are mentioned as having a

> *[…]very tangible effect for a company that wants to invest in security technologies. The security industry has to be sure that its products will be compatible with the general opinion of the public. The commercialisation of their new technologies would otherwise be impossible. The financial and human efforts that go into the development and production of a security product can therefore be easily wasted.*[59]

4.6.6 Barrier: lack of standardization

Another important barrier to development and use of both security-enhancing and privacy-enhancing technologies is a lack of standardization.[60] There are several related issues that act as barriers in this: the lack of a clear or commonly held definition of what 'security' and 'privacy' entails in practice; uncertainty about legal obligations and a fragmented regulatory landscape in the EU with regards to privacy and security; and incompatibility of different kinds of technological solutions with existing systems or other solutions. Some examples of where lack of standardization hinders technology development and use are a lack of common technical and interoperability standards for automated border control systems, as well as standards for biometric identifiers, or a lack of standards for communication interoperability.[61]

For privacy this issue is more pronounced than for security: as privacy is a relatively new issue many companies do not have extensive experience with best practices are sparse and reliable knowledge of what precisely to do to enhance privacy is hard to come by.

---

[57] European Commission, "Commission Staff Working Document on Transport Security ", SWD(2012) 143 final Brussels, 2012.
[58] van Lieshout, et al., 2012.
[59] European Commission, "Security Industrial Policy: Action Plan for an Innovative and Competitive Security Industry", 2012.
[60] Ibid.; van Lieshout, et al., 2012.
[61] European Commission, "Security Industrial Policy: Action Plan for an Innovative and Competitive Security Industry", 2012.

4.6.7 Barrier: reactive, not proactive approach

Organizations tend to behave reactively and not proactively with regards to privacy protection and security. Similarly, governments tend to formulate regulations and mandatory requirements in response to issues that occur, and not in a proactive manner. Technologies that may not be applied because little attention to security or privacy issues was given during the design stage of products and services. The alternative to such reactive approaches are usually described as 'security by design' and 'privacy by design', for example by Ann Cavoukian, the Information Commissioner of Ontario, Canada.[62]

A reactive approach may still create a demand for technologies in order to 'patch up' security or privacy vulnerabilities in systems and services, but overall we expect that a proactive approach would increase demand for privacy enhancing and security enhancing technologies.[63]

4.7 Conclusion

In the previous sections we discussed a number of key drivers and barriers in the development and use of technologies for privacy and security. While this is a preliminary analysis (in task 2.2 of the PRISMS project, for example, some of these drivers and barriers will be examined in more detail in the sociotechnical analysis), it provides an overview of how technology development for security and privacy purposes differs:

Driver	Effect on technology development for security	Effect on technology development for privacy
Technology and industry push	Strong	Weak
Events with high societal impact	Strong	Weak
Government policy and regulation	Strong	Strong
Consumer demand	Strong	Strong

Table 6 – factors driving technology development and use

Barrier	Effect on technology development for security	Effect on technology development for privacy
Lack of standardization	Strong	Strong
Not a unique selling point	Average	Strong
Reactive approach	Average	Strong

Table 7 – factors hindering technology development and use

Overall these tables suggest that technology development for security is subject to a number of drivers that are mostly absent for privacy: a technology and industry push, and events with a high societal impact. In addition, the relatively new field of privacy protection technologies suffers from a number of barriers that are less pronounced in the more established fields of security protection technologies: the idea that privacy is not a unique selling point, and a mostly reactive approach to the use of such technologies by consumers and organizations.

[62] Cavoukian, Ann, "Privacy by Design: The 7 Foundational Principles ", Information and Privacy Commissioner of Ontario, Toronto, 2011.
[63] European Commission, "Security Industrial Policy: Action Plan for an Innovative and Competitive Security Industry", 2012; van Lieshout, et al., 2012.

5 CONCLUSION

In the previous chapter we assessed for a series of key technological domains the fit for privacy or security purposes of technologies in each domain, the impact of the use of these technologies in practice, and drivers and barriers in the development of technologies for security and privacy.

The assessment of different technology domain fit for purpose and impact in practice was summarized in Table 5 in the previous chapter. The assessment suggests that a trade-off exists between security and privacy that appears to be inherent in technology development and use. Increased investments in technologies that have a positive impact on security tend to simultaneously have a negative impact on privacy. Some notable exceptions exist, however: the fields of information security and human sciences do not show such a trade-off.

A trade-off between privacy and security is also visible with regards to privacy protection technologies, especially when it comes to security by internet surveillance. Technologies specifically developed to enhance anonymity and to secure communications (showing an overlap with the information security domain) are perceived by some reports as having a negative impact on security through surveillance.

Technology development is subject to factors that drive it or hinder it, influencing how the trade-off between security and privacy turns out. The drivers and barriers outlined in Table 6 and Table 7 in the previous chapter suggest that technology development for security is subject to a number of drivers that are mostly absent for privacy: a technology and industry push, and events with a high societal impact. In addition, the relatively new field of privacy protection technologies suffers from a number of barriers that are less pronounced in the more established fields of security protection technologies: the idea that privacy is not a unique selling point, and a mostly reactive approach to the use of such technologies by consumers and organizations.

One of the end results of the PRISMS project is a decision support system that will provide users (those who deploy and operate security systems) insight into the pros and cons, constraints and limits of specific security investments compared to alternatives taking into account a wider society context. While this preliminary analysis lacks nuance and detail, we identified a starting point for a decision support system on investments in security and privacy technologies, which may be based on the summarizing tables on technology domains, drivers and barriers listed above.

The results described in this deliverable are preliminary; based on the other activities performed in the same work package and in other work packages the results will be improved further, and eventually integrated into a final report on current developments on security and privacy technologies including studies on the mutual shaping processes between developers, users and uses of security and privacy technologies. With this preliminary deliverable we lay a foundation for the work done in the other activities in the PRISMS project that often relate to technology, including a policy assessment, a criminological analysis, a legal perspective, a discourse analysis of media attention to privacy, security and trust issues, an analysis of existing public opinion surveys, and a survey of citizens' privacy and security perceptions.

REFERENCES

Akrich, Madeleine, "The description of technical objects", in Wiebe Bijker, and John Law (eds.), *Shaping Technology/Building Society: Studies in Sociotechnical Change*, MIT Press, Cambridge, Mass, 1992, pp. 205-224.

Article 29 Data Protection Working Party, "Working document on data protection issues related to RFID technology", 10107/05/EN, WP 105, Brussels, 2005.

Buttarelli, Giovanni, "Welcome address: Fundamental rights at stake", Paper presented at: EDPS Workshop on Video-surveillance with in Community institutions and bodies Brussels, 2009. http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2009/09-09-30_videosurveillance_welcome_address_EN.pdf

Buttarelli, Giovanni, "Legal Restrictions – Surveillance and Fundamental Rights", Paper presented at: Conference on New Technical Means of Surveillance and the Protection of Fundamental Rights - Challenges for the European Judiciaries, Vienna, 2009. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2009/09-06-19_Vienna_surveillance_EN.pdf

Buttarelli, Giovanni, "The Surveillance Policy in Europe, Today and Tomorrow", Paper presented at: The Conference for the 30th Anniversary of the CRID, Namur, Belgium, 2010. http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2010/10-01-22_Namur_surveillance_EN.pdf

Cavoukian, Ann, "Privacy by Design: The 7 Foundational Principles ", Information and Privacy Commissioner of Ontario, Toronto, 2011. http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf

"Check Point 2013 Annual Security Report", Check Point Software Technologies Ltd., Tel Aviv; San Carlos, Cal., 2013. http://sc1.checkpoint.com/documents/security-report/files/assets/common/downloads/publication.pdf

"Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC", *Official Journal of the European Union L 105*, Vol. 49, 15.3.2006, pp. 54-63. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF

ENISA (European Network and Information Security Agency), "National Cyber Security Strategies - Setting the Course for National Efforts to Strengthen Security in Cyberspace", May, Heraklion, Crete, 2012. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper/at_download/fullReport

ESRAB (European Security Research Advisory Board), "Meeting the challenge: the European Security Research Agenda. A report from the European Security Research Advisory Board", Office for Official Publications of the European Communities, Luxembourg, 2006. http://ec.europa.eu/enterprise/policies/security/files/esrab_report_en.pdf

European Commission, "The EU Internal Security Strategy in Action: Five steps towards a more secure Europe", COM(2010) 673 final., Brussels, 2010.

European Commission, "Commission Staff Working Document on Transport Security ", SWD(2012) 143 final Brussels, 2012. http://ec.europa.eu/transport/themes/security/doc/2012-05-31-swd-transport-security.pdf

European Commission, "Security Industrial Policy: Action Plan for an Innovative and Competitive Security Industry", COM(2012) 417 final Brussels, 2012. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0417:FIN:EN:PDF

European Security Research & Innovation Forum (ESRIF), "ESRIF Final Report", Brussels, 2009. http://ec.europa.eu/enterprise/policies/security/files/esrif_final_report_en.pdf

Finn, Rachel L., and David Wright, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", *Computer Law & Security Review*, Vol. 28, No. 2, 2012, pp. 184-194.

Finn, Rachel L., David Wright, and Michael Friedewald, "Seven types of privacy", in Serge Gutwirth, Ronald Leenes, Paul De Hert, and Yves Poullet (eds.), *European Data Protection: Coming of Age*, Springer, Dordrecht, 2013, pp. 3-32.

Friedewald, Michael, David Wright, Kush Wadhwa, Serge Gutwirth, Marc van Lieshout, Gabriela Bodea, Charles D. Raab, Iván Székely, Irma van der Ploeg, Gideon Skinner, Simone Kimpeler, Jana Schuhmacher, Kerstin Goos, Rachel Finn, Monica Lagazio, Kristof Verfaillie, Gloria González Fuster, Anne Fleur van Veenstra, Erik Uszkiewicz, Jason Pridmore, and Govert Valkenburg, "Central Concepts and Implementation Plan", PRISMS Deliverable 1.1, December 2012.

Galbraith, John Kenneth, *The New Industrial State*, Houghton Mifflin, Boston, 1971.

Gilbert, Nigel, Anne Anderson, James Backhouse, David Birch, Brian Collins, William Dutton, John Edwards, Ian Forbes, Wendy Hall, Andy Hopper, Cliff Jones, and Martyn Thomas, "Dilemmas of Privacy and Surveillance: Challenges of Technological Change", The Royal Academy of Engineering, London, 2007.

Green, Nicola, "On the Move: Technology, Mobility and the Mediation of Social Time and Space", *The Information Society: An International Journal*, Vol. 18, No. 4, 2002, pp. 281–292.

Gutwirth, Serge, Rocco Bellanova, Michael Friedewald, Dara Hallinan, David Wright, Paul McCarthy, Julien Jeandesboz, Emilio Mordini, Silvia Venier, Marc Langheinrich, and Vlad Coroama, "Smart Surveillance - State of the Art Report", Deliverable 1, SAPIENT Project, January 2012. http://www.sapientproject.eu/docs/D1.1-State-of-the-Art-submitted-21-January-2012.pdf

Hayes, Ben, "Arming Big Brother: The EU's Security Research Programme", TNI Briefing Series No. 2006/1, Transnational Institute; Statewatch, Amsterdam, 2006. http://www.statewatch.org/analyses/bigbrother.pdf

INFOSEC Research Council, "Hard Problem List", 2005. http://www.cyber.st.dhs.gov/docs/IRC_Hard_Problem_List.pdf

Jo, Whasun, "Global Political Economy of Technology Standardization: A Case of the Korean Mobile Telecommunications Market", *Telecommunications Policy*, Vol. 31, No. 2, 2007, pp. 124–138.

van Lente, Harro, and Arie Rip, "Expectations in Techological Developments: An Example of Prospective Structures to Be Filled in by Agency", in Barend van der Meulen, and

Cornelis Disco (eds.), *Getting New Technologies Together: Studies in Making Socio-technical Order*, de Gruyter, New York, 1998, pp. 203–230.

van Lieshout, Marc, Linda Kool, Gabriela Bodea, James Schlechter, and Bas van Schoonhoven, "Stimulerende En Remmende Factoren Van Privacy by Design in Nederland", TNO, Delft, 2012.

Martí Sempere, Carlos, "The European Security Industry: A Research Agenda", Economics of Security Working Paper 29, German Institute for Economic Research, Berlin, 2010. http://www.diw.de/documents/publikationen/73/diw_01.c.354173.de/diw_econsec0029.pdf

Moore, Gordon E., "Cramming More Components Onto Integrated Circuits", *Electronics*, Vol. 38, No. 8, 1965, pp. 114-117.

Oudshoorn, Nelly, and Trevor Pinch (eds.), *How Users Matter: The Co-Construction of Users and Technology*, MIT Press, Cambridge, Mass. and London, 2003.

Parry, Richard, "Episteme and Techne", in Edward N. Zalta (ed.), *The Stanford Encyclopedia of Philosophy (Fall 2008 Edition)*, Stanford, Cal., 2007. http://plato.stanford.edu/entries/episteme-techne/

Solove, Daniel J., *Understanding privacy*, Harvard University Press, Cambridge, Mass., 2008.

The Irish Council for Bioethics, "Biometrics: Enhancing Security or Invading Privacy?", Dublin, 2009. http://irishpatients.ie/news/wp-content/uploads/2012/04/Irish-Council-Bioethics-Final_Biometrics_Doc_HighRes.pdf

Warren, Samuel D., and Louis D. Brandeis, "The Right To Privacy", *Harvard Law Review*, Vol. 4, No. 5, 1890, pp. 193-220.

Westin, Alan F., *Privacy and freedom*, Atheneum, New York, 1967.

Wright, David, Iván Székely, Michael Friedewald, Rowena Rodriguez, Reinhard Kreissl, Johann Čas, Charles Raab, Beatrix Vissy, Kerstin Goos, Charles Leleux, William Webster, Gemma Galdon Clavell, Clive Norris, Marija Krlic, Leroy Groves, Anthony Amicelle, Stefan Strauß, Kirstie Ball, Dara Hallinan, Paul De Hert, Antonella Galetta, and Richard Jones, "Surveillance, fighting crime and violence", IRISS Deliverable 1.1, December 2012. http://irissproject.eu/wp-content/uploads/2012/02/IRISS_D1_MASTER_DOCUMENT_17Dec20121.pdf

APPENDIX A – LITERATURE STUDY TEMPLATE

The literature review was performed by several members of the PRISMS project. To structure the review and to ensure consistency, we used a template that each member filled in for the documents that were studied. This template is shown below.

DOCUMENT DETAILS	**ST** **PT**
File name:	
Authors:	
Full title:	
Year of publishing:	
Institute/platform/organization (if any):	
Type of document: Research report / technology roadmap / policy document / …	
Country/Area:	
Keywords:	
DESCRIPTIVES	
Purpose and scope of the document	
Privacy and/or security technologies covered	
Domain in which the technologies are applied	
Societal challenges addressed by the technologies	
ANALYSIS	
Type of privacy or security addressed (according to the classification of the inception report)	
Privacy and / or security technologies covered and their interference	
Stakeholders or actors involved; impact assessment of the technologies	
General interpretation and relevance	

APPENDIX B - LITERATURE STUDY DOCUMENT LIST

As described in chapter 2, we performed an extensive literature study during this study. Part of these documents are listed in the list of references. Here we provide an overview of the documents that were studied. To reduce the length of the list, the references are provided in an abbreviated format.

Research reports and papers

1. Auffermann, B. & Kaskinen, J. (eds.) (FFRC) (2010) Security in futures – Security in change Proceedings of the conference.
2. Bioetics (2009) Biometrics enhancing security or invading privacy.
3. Buttarelli (EPDS) (2009) Keynote on Legal Restrictions – Surveillance and Fundamental Rights.
4. Buttarelli (EPDS) (2010) Keynote on The Surveillance policy in Europe, today and tomorrow.
5. Cameo Wood (2003) Privacy issues and privacy enhancing technologies.
6. Cavoukian, A. (2008) Privacy and video surveillance in mass transit systems: a special investigation report.
7. Che Yen Wen (2005) Mask Detection at ATM by CCTV.
8. CRS (2001) aviation security technologies and procedures screening passengers and baggage.
9. Cyberspace Law and Policy Center (2008) Distinguishing PETs from PITs: Developing technology with privacy in mind.
10. Dutch Ministry of science technology and innovation – META Group (2005) Privacy enhancing technologies.
11. ENISA (2008) Study on data collection and storage in the EU.
12. ENISA (2011). Botnets: Detection, Measurement, Disinfection & Defence.
13. ENISA (2011). Managing Multiple Electronic Identities.
14. ENISA (2011). Privacy, Accountability and Trust – Challenges and Opportunities.
15. ENISA (2011). Protecting Industrial Control Systems. Recommendations for Europe and Member States (81 pages) Research studies.
16. ENISA (2012). National Cybersecurity Strategy.
17. ESRAB (2006) Meeting the challenge: the European Security Research Agenda – A report from the European Security Research Advisory Board
18. European Commission (2010) FORESEC: European security in light of evolving trends, drivers and threats.
19. European Security Research & Innovation Forum (ESRIF). (2009) Final report.
20. Forensic SCIENCE magazine (2005) The mask detection technology for occluded face analysis in the surveillance system.
21. Fraunhofer/IPTS (2003) Science and technology road mapping: ambient intelligence in everyday life.
22. Future of identity in the information society (FIDIS) project reports.
23. Garfinkel (2010) Digital forensics research the next 10 years.
24. IPTS (2003) Security and privacy for the citizen in the post-September 11 digital age: a prospective overview.
25. IPTS (2007) RFID Technologies: Emerging Issues, Challenges and Policy Options
26. IPTS (2008) Large scale biometrics deployment

27. IPTS (2012) Pan-European Survey of Practices, Attitudes and Policy Preferences as regards Personal Identity Data Management
28. IST-PAMPAS (2003). Pioneering advanced mobile privacy and security.
29. Jones Randell (2004) Dependable pervasive systems.
30. Kevin Aquilina (2010). Public security versus privacy in technology law: A balancing act?
31. National Research Council (2007). Protecting individual privacy in the struggle against terrorism. A Framework for Program Assessment.
32. NISTEP (2003) Privacy issues and privacy enhancing technologies.
33. O'Hara Shadbolt (2004) Knowledge technologies and the semantic web.
34. PATS (2010) Combined national reports and cross-national report on privacy awareness of security organizations
35. PATS (2010) Mapping the security regimes.
36. PATS (2010) Report on the usefulness of ethically focused brand indicators as a means of managing the balance between security and privacy.
37. PISA consortium (2003) Handbook of privacy and privacy-enhancing technologies: the case of intelligent software agents.
38. PRISE (2008) Preparatory action on the enhancement of the European industrial potential in the field of Security research.
39. Raab (2004) The future of privacy
40. RAND (2007) The strategic challenge of border security
41. Royal Academy of Engineering (2007). Dilemmas of privacy and surveillance
42. RSA laboratories (2005). RFID security and privacy: a research survey.
43. Saadawi & Jordan (eds.) (2011) Cyber infrastructure protection.
44. Sasse (2004) Usability and trust in information systems
45. SENSATION (2004). Data security and privacy: guidelines and European roadmap.
46. Surveillance Studies Network (2006) A report on the surveillance society.
47. SWAMI project (2006) Final report.
48. The royal academy of engineering (2007) Dilemmas of privacy and surveillance: challenges of technological change.
49. Tully (2010) Pervasive computing.
50. University of Lodz (2008) Combined national reports and cross-national report on privacy awareness of security organizations.

Technology roadmaps

1. ASU-IP Commissioner Ontario (2010) The roadmap for privacy by design in mobile communications: a practical tool for developers, service providers, and users.
2. BIOVISION (2003) Roadmap for biometrics in Europe .
3. BRIDGE (2009) Security technology roadmap.
4. CABA (2002) Technology Roadmap for Intelligent buildings.
5. CWI (center for mathematics and informatics) (2003) Biovision: Roadmap for biometrics in Europe to 2010.
6. Forskningsradet RFID Technology Resource Network (2008) RFID Technology Roadmap
7. Homeland security (2009) A roadmap for cybersecurity research.
8. Infocomm (2002) Security Technologies for eCommerce.
9. Information society technologies (2012) Roadmap for Advanced Research in Privacy and Identity Management (RAPID)
10. MITRE (2008) State of the Art Biometrics Excellence Roadmap.

11. NPIA (2006) Automated face recognition: applications within law enforcement. Market and technology review.
12. PCI Security standards council (2010) Initial Roadmap: Point-to-point encryption technology and PCI DSS compliance.
13. RFID-RNET (2008). RFID technology roadmap: Wireless smart systems and RFID.
14. Sun Dong Tan (2009) Technology roadmap for smart iris recognition.
15. VTT (2007) Technology roadmap of security research.
16. Wolfram, Gampl & Gabriel (eds.) (2008). The RFID Roadmap: the next steps for Europe.

Policy and foresight documents

1. ACPO National ANPR User group (2004) Automatic number plate recognition: denying criminals use of the road.
2. Auffermann, B. & Luoto, L. (FFRC) (2009) Foresight of evolving security threats posed by emerging technologies (FESTOS) WP3 Emerging treats – D3.3 Integrated Security Threats report
3. Congressional research service (2001) Aviation security technologies and procedures: Screening passengers and baggage.
4. CSIS (2010) Industry towards security
5. CSIS (2012) Global forecast risk opportunity and the next administration. Foresight of security risks and the consequences for defense (US).
6. Dutch Ministry of the Interior (2004) Whitepaper on PET for decision-makers.
7. Foresight (2004) Cyber trust and crime prevention (CTPC project) technology forward look.
8. Foresight (UK-OST) Technology and innovation futures: UK Growth opportunities for the 2020s.
9. Foresight CTCP (2004) Gaining insight from three different futures.
10. Homeland security (2010) Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland.
11. Infosec Research Council (2005) Hard problems.
12. Interpol (2009) Handbook on DNA data exchange and practice
13. IP Privacy officer Ontario (2002) Security technologies Enabling Privacy (STEPS): Time for a paradigm shift.
14. National Research Council (2008) Protecting individual privacy in the struggle against terrorists
15. NISTEP (2010) Contribution of science and technology to future society – summary of the 9th science and technology foresight.